PCT

日本国特許庁
JAPAN PATENT OFFICE

27.4.2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

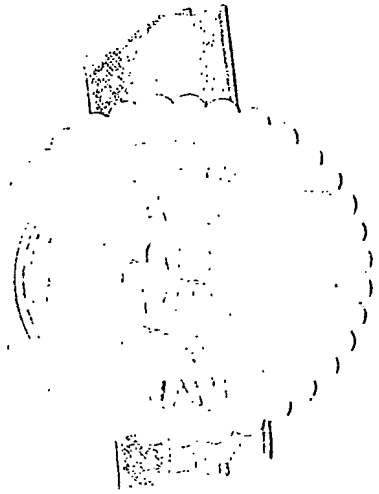
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　５月　９日

出願番号
Application Number: 特願２００３－１３１００５

[ST. 10/C]: [ＪＰ２００３－１３１００５]

出願人
Applicant(s): 日本電気株式会社



PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

２００４年　３月　２日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号　出証特２００４－３０１５７１１

【書類名】　特許願
【整理番号】　35001200
【提出日】　平成15年 5月 9日
【あて先】　特許庁長官殿
【国際特許分類】　H04L 9/00
H04B 7/26
H04L 9/32
【発明者】
【住所又は居所】　東京都港区芝五丁目７番１号　日本電気株式会社内
【氏名】　田口　大悟
【発明者】
【住所又は居所】　東京都港区芝五丁目７番１号　日本電気株式会社内
【氏名】　楫　勇一
【発明者】
【住所又は居所】　東京都港区芝五丁目７番１号　日本電気株式会社内
【氏名】　野田　潤
【特許出願人】
【識別番号】　000004237
【氏名又は名称】　日本電気株式会社
【代理人】
【識別番号】　100097157
【弁理士】
【氏名又は名称】　桂木　雄二
【手数料の表示】
【予納台帳番号】　024431
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9303562

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　デジタル情報の流通制御方法および流通制御システム

【特許請求の範囲】

【請求項１】　デジタル情報の配信サービスを行うサーバと、前記デジタル情報の配信サービスを受ける情報処理端末と、を有するシステムにおけるデジタル情報の流通制御方法において、

前記デジタル情報とデータ転送制御条件を示す流通制御情報とを含む配信データを前記サーバから前記情報処理端末へ配信し、

前記情報処理端末に前記配信データを格納し、

前記流通制御情報に従って前記情報処理端末と他の情報処理端末との間での前記配信データを含む情報の転送を制御する、

ことを特徴とするデジタル情報の流通制御方法。

【請求項２】　前記転送制御では、

前記情報処理端末の固有情報を用いて生成された前記配信データを含む情報を前記他の情報処理端末へ転送して格納し、

前記他の情報処理端末に格納された配信データを含む情報を前記情報処理端末へ再格納する前に、前記流通制御情報に従って前記情報処理端末への再格納の可否を判定する、

ことを特徴とする請求項１記載の流通制御方法。

【請求項３】　前記転送制御では、

前記情報処理端末の固有情報を用いて生成された前記配信データを含む情報を前記他の情報処理端末へ転送して格納し、

前記他の情報処理端末に格納された配信データを含む情報を前記情報処理端末へ再格納する前に、前記流通制御情報に従って前記サーバへの問合せの可否を判定する、

ことを特徴とする請求項１記載の流通制御方法。

【請求項４】　前記流通制御情報は、前記配信データを含む情報の転送可否決定条件および前記サーバへの問合せの可否決定条件のうち少なくとも１つを含むことを特徴とする請求項１記載の流通制御方法。

【請求項５】　デジタル情報の配信サービスを行うサーバと、前記デジタル情報の配信サービスを受ける情報処理端末とを有するシステムにおけるデジタル情報の流通制御方法において、

前記デジタル情報とデータ転送制御条件を示す流通制御情報とを含む配信データを前記サーバから前記情報処理端末へ配信し、

前記情報処理端末に前記配信データを格納し、

前記情報処理端末に割り当てられた端末固有情報を用いて前記配信データを含む第１安全化データを生成して他の情報処理端末へ転送し、

前記他の情報処理端末に格納された安全化データに含まれる配信データを前記情報処理端末へ再格納する前に、安全化データ送信要求を前記他の情報処理端末へ送信し、

前記情報処理端末の端末固有情報と、前記安全化データ送信要求に対応する第２安全化データに含まれる端末固有情報および流通制御情報とに基づいて、当該第２安全化データに含まれる配信データを前記情報処理端末へ再格納可能か否かを判定し、

再格納可能であるときに前記第２安全化データに含まれる前記配信データを前記情報処理端末に格納する、

ことを特徴とするデジタル情報の流通制御方法。

【請求項６】　前記流通制御情報は、安全化データの転送可否決定条件および前記サーバへの問合せの可否決定条件のうち少なくとも１つを指示することを特徴とする請求項５記載の流通制御方法。

【請求項７】　前記第２安全化データの流通制御情報によりサーバ問合せが指定されている場合には、当該第２安全化データおよび前記安全化データ送信要求を含む安全化データ問合せを前記サーバに対して送信することを特徴とする請求項６記載の流通制御方法。

【請求項８】　前記サーバは、

前記安全化データ問合せを受信すると、前記安全化データ問合せに含まれる第２安全化データの更新可否を判定し、

更新可能な場合には、当該サーバに割り当てられたサーバ固有情報を用いて当

該第２安全化データを更新した更新安全化データを生成し、当該更新安全化データを前記安全化データ問合せに対する応答として返送し、

前記情報端末は、前記更新安全化データを前記安全化データ送信要求に対応する第２安全化データとして受信することを特徴とする請求項７記載の流通制御方法。

【請求項９】　前記更新安全化データは有効期限情報を含み、

前記情報処理端末は、前記情報処理端末の端末固有情報と前記第２安全化データに含まれる端末固有情報、有効期限情報および流通制御情報とに基づいて、当該配信データを前記情報処理端末へ再格納可能か否かを判定する、

ことを特徴とする請求項８記載の流通制御方法。

【請求項１０】　前記情報処理端末は、さらに、前記安全化データ送信要求に当該要求特定情報を付加して前記他の情報処理端末へ送信し、

前記サーバは前記更新安全化データに前記要求特定情報を含めて返送し、

前記情報処理端末は、前記情報処理端末の端末固有情報と前記第２安全化データに含まれる端末固有情報、要求特定情報および流通制御情報とに基づいて、当該配信データを前記情報処理端末へ再格納可能か否かを判定する、

ことを特徴とする請求項８記載の流通制御方法。

【請求項１１】　前記要求特定情報は、前記データ送信要求時に発生した乱数であることを特徴とする請求項１０記載の流通制御方法。

【請求項１２】　前記流通制御情報は、データ転送の可否決定条件、情報転送時の暗号化の要否決定条件、および、前記サーバへの問合せの可否決定条件のうち少なくとも１つを指示することを特徴とする請求項５記載の流通制御方法。

【請求項１３】　前記端末固有情報は、流通署名作成鍵、流通署名検証鍵、端末証明書、暗号化鍵、暗号化鍵証明書、復号鍵、および、識別情報のうち少なくとも前記識別情報を含むことを特徴とする請求項１２記載の流通制御方法。

【請求項１４】　前記情報処理端末は、

前記流通制御情報がデータ転送時の暗号化を指示している場合は、前記端末固有情報に含まれる前記暗号化鍵を用いて前記配信データに含まれるデジタル情報を暗号化し、

暗号化されたデジタル情報を含む配信データを用いて前記第１安全化データを生成して前記他の情報処理端末へ転送し、

前記第２安全化データに含まれる前記配信データの暗号化されたデジタル情報を前記端末固有情報に含まれる前記復号鍵を用いて復号する、

ことを特徴とする請求項１３記載の流通制御方法。

【請求項１５】　デジタル情報の配信サービスを行うサーバから前記デジタル情報の配信を受け、バックアップ用の他の情報処理端末との間でデータ転送可能な携帯情報端末において、

データ転送を制限する条件を示す流通制御情報と前記デジタル情報とを含む配信データを前記サーバから受信し格納する配信データ格納手段と、

当該携帯情報端末に割り当てられた端末固有情報を格納する端末固有情報格納手段と、

前記配信データ格納手段から前記他の情報処理端末へ前記配信データを転送するために、前記端末固有情報を用いて前記配信データを含む第１安全化データを生成し、前記他の情報処理端末へ送信する安全化データ生成手段と、

前記他の情報処理端末から第２安全化データを受信して当該第２安全化データに含まれる配信データを前記配信データ格納手段へ再格納する前に、前記他の情報処理端末へデータ送信要求を行うデータ送信要求生成手段と、

前記データ送信要求の応答として前記他の情報処理端末から前記第２安全化データを受信すると、当該携帯情報端末の前記端末固有情報と前記第２安全化データに含まれる端末固有情報および流通制御情報とを用いて、当該第２安全化データが再格納可能か否かを検証し、再格納可能であるときに前記第２安全化データに含まれる配信データを前記配信データ格納手段に格納する安全化データ検証手段と、

を有することを特徴とする携帯情報端末。

【請求項１６】　さらに、

前記データ送信要求の応答として前記他の情報処理端末から前記第２安全化データを受信すると、当該携帯情報端末の前記端末固有情報と前記第２安全化データに含まれる端末固有情報および流通制御情報とを用いて、当該第２安全化デー

タの前記配信データ格納手段への転送可否を判定する判定手段を有し、

前記第２安全化データを前記配信データ格納手段への転送可能であれば、前記安全化データ検証手段により当該第２安全化データが再格納可能か否かを検証することを特徴とする請求項１５記載の携帯情報端末。

【請求項１７】　前記流通制御情報は、データ転送の可否決定条件および前記サーバへの問合せの可否決定条件のうち少なくとも１つを指示することを特徴とする請求項１６記載の携帯情報端末。

【請求項１８】　前記判定手段は、前記第２安全化データの流通制御情報によりサーバ問合せが指定されている場合には、前記データ送信要求および前記第２安全化データを含む安全化データ問合せを前記サーバに対して送信することを特徴とする請求項１７記載の携帯情報端末。

【請求項１９】　情報処理端末に対してデジタル情報の配信サービスを行うサーバにおいて、

当該サーバに割り当てられたサーバ固有情報を格納するサーバ固有情報格納手段と、

前記デジタル情報とデータ転送制御条件を示す流通制御情報とを含む配信データを生成して前記情報処理端末へ配信する配信データ管理手段と、

前記情報処理端末の端末固有情報および要求された安全化データを含む安全化データ問合せを受信すると、当該安全化データ問合せに含まれる前記安全化データの更新可否を判定し、更新可能な場合に当該安全化データを更新して前記安全化データ問合せの応答として返送する安全化データ更新手段と、

を有することを特徴とするサーバ。

【請求項２０】　データ転送を制限する条件を示す流通制御情報とデジタル情報とを含む配信データをサーバから受信する携帯情報端末と接続可能であり、前記携帯情報端末が受信した前記配信データをバックアップする情報処理装置であって、

前記携帯情報端末に割り当てられた端末固有情報を用いて生成された前記配信データを含む第１安全化データを格納する安全化データ格納手段と、

前記安全化データ格納手段に格納された第１安全化データに含まれる配信デー

タを前記携帯情報端末へ再格納するための安全化データ送信要求を前記携帯情報端末から受信し、当該受信したデータ送信要求と前記安全化データ格納手段に格納された第１安全化データの端末固有情報および流通制御情報とに基づいて、当該格納された第１安全化データを第２安全化データとして前記携帯情報端末へ返送するか否かを判定する判定手段と

を有することを特徴とする情報処理装置。

【請求項２１】　デジタル情報の配信サービスを行うサーバと、前記デジタル情報の配信を受ける第１情報処理端末と、前記第１情報処理端末との間でデータ転送可能な第２情報処理端末と、を少なくとも有する流通制御システムにおいて、

前記サーバは、データ転送を制限する条件を示す流通制御情報を前記デジタル情報に付加した配信データを生成して前記第１情報処理端末へ送信する配信データ管理手段を少なくとも有し、

前記第１情報処理端末は、

前記配信データを格納する配信データ格納手段と、

前記第１情報処理端末に割り当てられた端末固有情報を格納する端末固有情報格納手段と、

前記配信データ格納手段から前記第２情報処理端末へ前記配信データを転送するために、前記端末固有情報を用いて前記配信データを含む第１安全化データを生成し、前記第２情報処理端末へ送信する安全化データ生成手段と、

前記第２情報処理端末から第２安全化データを受信して当該第２安全化データに含まれる配信データを前記配信データ格納手段へ再格納するために、前記第２情報処理端末へデータ送信要求を行うデータ送信要求生成手段と、

前記データ送信要求の応答として前記第２情報処理端末から前記第２安全化データを受信すると、前記端末固有情報を用いて当該第２安全化データが再格納可能か否かを検証し、再格納可能であるときに前記第２安全化データに含まれる配信データを前記配信データ格納手段に格納する安全化データ検証手段と、を少なくとも有し、

前記第２情報処理端末は、

前記第１情報処理端末から転送された前記第１安全化データを格納する安全化データ格納手段と、

前記データ送信要求と前記安全化データ格納手段に格納された安全化データの端末固有情報および流通制御情報とに基づいて、当該格納された安全化データを第２安全化データとして前記第１情報処理端末へ返送するか否かを判定する判定手段と、を少なくとも有する、

ことを特徴とする流通制御システム。

【請求項２２】　コンピュータに、情報処理端末に対してデジタル情報の配信サービスを行うサーバ機能を実現するためのサーバプログラムにおいて、

前記デジタル情報とデータ転送制御条件を示す流通制御情報とを含む配信データを生成して前記情報処理端末へ配信するステップと、

前記情報処理端末の端末固有情報および要求された安全化データを含む安全化データ問合せを受信すると、当該安全化データ問合せに含まれる前記安全化データの更新可否を判定するステップと、

更新可能な場合に当該安全化データを更新して前記安全化データ問合せの応答として返送するステップと、

を有することを特徴とするサーバプログラム。

【請求項２３】　コンピュータに、デジタル情報の配信サービスを行うサーバから前記デジタル情報の配信を受けると共にバックアップ用の他の情報処理端末との間でデータ転送を実行させる携帯情報端末用のプログラムにおいて、

データ転送を制限する条件を示す流通制御情報と前記デジタル情報とを含む配信データを前記サーバから受信し格納するステップと、

前記他の情報処理端末へ前記配信データを転送するために、前記端末固有情報を用いて前記配信データを含む第１安全化データを生成し、前記他の情報処理端末へ送信するステップと、

前記他の情報処理端末から第２安全化データを受信して当該第２安全化データに含まれる配信データを前記配信データ格納手段へ再格納する前に、前記他の情報処理端末へデータ送信要求を行うステップと、

前記データ送信要求の応答として前記他の情報処理端末から前記第２安全化デ

ータを受信すると、当該携帯情報端末の前記端末固有情報と前記第２安全化データに含まれる端末固有情報および流通制御情報とを用いて、当該第２安全化データが再格納可能か否かを検証するステップと、

再格納可能であるときに前記第２安全化データに含まれる配信データを格納するステップと、

を有することを特徴とする携帯情報端末用のプログラム。

【請求項２４】　前記データ送信要求の応答として前記他の情報処理端末から前記第２安全化データを受信すると、当該携帯情報端末の前記端末固有情報と前記第２安全化データに含まれる端末固有情報および流通制御情報とを用いて、当該第２安全化データの前記配信データ格納手段への転送可否を判定するステップと、

前記第２安全化データを前記配信データ格納手段への転送可能であれば、前記安全化データ検証手段により当該第２安全化データが再格納可能か否かを検証するステップと、

を更に有することを特徴とする請求項２３記載の携帯情報端末用のプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明はデジタル情報への不正なアクセスを防止するためのデジタル情報管理技術に係り、特に提供されるサービスに対する不正アクセスの防止とサービス利用者の利便性とを考慮したデジタル情報流通制御システムおよび方法に関する。

【０００２】

【従来の技術】

近年、デジタルコンテンツ配信サービスが普及し、アプリケーションソフト、音楽、映像、雑誌、チケットなどもネットワークを通して配信されるようになってきた。このようなコンテンツは著作物や商品であるから、どのように保護するかはますます重要な課題となっている。

【０００３】

たとえば、携帯電話機の着信メロディを配信するサービスでは、その著作権を保護する技術としてＳＭＡＦ(Synthetic music Mobile Application Format)が主に採用されている。ＳＭＡＦはヤマハ株式会社が設計したデータフォーマット仕様であり、主に携帯情報端末や携帯電話機で再生するマルチメディアコンテンツのデータ形式を定義するために用いられる。ＳＭＡＦによれば、ＳＭＡＦデータに（Ａ）保存可・転送可、（Ｂ）保存可・転送不可、（Ｃ）保存不可・転送不可の３つのコピーステータス（Ｃｏｐｙ　Ｓｔａｔｕｓ）を設定することができる。したがって、コピーステータスに応じて、データの保存や他の携帯電話機への転送が可能／不可能となり、不正なデータ転送などを防止することができる。

【０００４】

このように携帯電話機にダウンロートしたコンテンツは、携帯電話機を交換したときあるいは操作ミスなどで消失したときのために、ユーザのパーソナルコンピュータなどにバックアップをとっておくことが望ましい。しかしながら、バックアップを無制限に認めることは正当な使用者以外の者に違法コピーされる可能性も有しているために、サービス提供者としては著作権保護も併せて考慮しなければならない。

【０００５】

特開２００２－１８５５７９号公報（特許文献１）には、このような著作権保護を考慮したバックアップ方法が開示されている。この従来の方法では、携帯電話機からパーソナルコンピュータへＪＡＶＡ(登録商標）アプリケーションをバックアップする際に携帯電話機の製造番号と電話番号とを付加し、復元する際に携帯電話機の製造番号および／または電話番号を比較することで、ＪＡＶＡ（登録商標）アプリケーションの不正使用を防止する。

【０００６】

また、データの改ざんの有無を検知するデジタル署名技術やデータの不正閲覧や盗聴を防止する暗号技術などを用いることでバックアップやリストア時のデータ保護を図ることも可能である。

【０００７】

【特許文献１】

特開２００２－１８５５７９号公報（段落番号００１８～００２３、００２６～００２８、図４）。

【０００８】

【発明が解決しようとする課題】

しかしながら、上記従来のバックアップ方法にデジタル署名あるいは暗号化技術を組み合わせても、次のようなデータ不正使用を防止することはできない。たとえば、サービス利用者は残数１０回の電子チケットをサービス提供者から受信し、携帯電話機に格納する。この電子チケットは、対応するサービスを享受する度に１回ずつ残数が減るような電子チケットである。サービス利用者は、上記従来のバックアップ方法により残数１０回の電子チケットをパーソナルコンピュータへバックアップする。次に、携帯電話機を用いて通常の手順で１０回のサービスを享受する。その後、バックアップデータを携帯電話機に復元する。この場合、同じ携帯電話機であるから正常にリストアされる。したがって、この携帯電話機は、残数１０回の電子チケットが正常にリストアされ、再びサービス利用可能状態となってしまう。

【０００９】

このように従来技術では、携帯情報端末や携帯電話機などの携帯通信機器へデジタルコンテンツや電子チケットを配信するサービス事業者の権利保護とサービスを享受するサービス利用者の利便性とを十分に両立させることができなかった。

【００１０】

そこで、本発明の目的は、サービス提供者の権利保護とサービス利用者の利便性とを共に確保することができるデジタル情報の流通制御システムおよび方法を提供することにある。

【００１１】

また、本発明の他の目的は、配信されたデータのバックアップおよびリストアの正当性を確実に判定することができるデジタル情報の流通制御システムおよび方法を提供することにある。

【００１２】

さらに、本発明のその他の目的は、配信されたデータをバックアップおよびリストアするための条件を柔軟に設定できるデジタル情報の流通制御システムおよび方法を提供することにある。

【００１３】

【課題を解決するための手段】

本発明による流通制御方法は、デジタル情報の配信サービスを行うサーバと、前記デジタル情報の配信サービスを受ける情報処理端末と、を有するシステムにおけるデジタル情報の流通制御方法であって、前記デジタル情報とデータ転送制御条件を示す流通制御情報とを含む配信データを前記サーバから前記情報処理端末へ配信し、前記情報処理端末に前記配信データを格納し、前記流通制御情報に従って前記情報処理端末と他の情報処理端末との間での前記配信データを含む情報の転送を制御する、ことを特徴とする。

【００１４】

前記転送制御は、前記情報処理端末の固有情報を用いて生成された前記配信データを含む情報を前記他の情報処理端末へ転送して格納し、前記他の情報処理端末に格納された配信データを含む情報を前記情報処理端末へ再格納する前に、前記流通制御情報に従って前記情報処理端末への再格納の可否を判定する、ことを特徴とする。あるいは、前記転送制御は、前記情報処理端末の固有情報を用いて生成された前記配信データを含む情報を前記他の情報処理端末へ転送して格納し、前記他の情報処理端末に格納された配信データを含む情報を前記情報処理端末へ再格納する前に、前記流通制御情報に従って前記サーバへの問合せの可否を判定する、ことを特徴とする。

【００１５】

前記流通制御情報は、望ましくは、前記配信データを含む情報の転送可否決定条件および前記サーバへの問合せの可否決定条件のうち少なくとも１つを含む。

【００１６】

本発明の一実施形態によれば、デジタル情報の配信サービスを行うサーバと、前記デジタル情報の配信サービスを受ける情報処理端末とを有するシステムにおけるデジタル情報の流通制御方法は、前記デジタル情報とデータ転送制御条件を

示す流通制御情報とを含む配信データを前記サーバから前記情報処理端末へ配信し、前記情報処理端末に前記配信データを格納し、前記情報処理端末に割り当てられた端末固有情報を用いて前記配信データを含む第１安全化データを生成して他の情報処理端末へ転送し、前記他の情報処理端末に格納された安全化データに含まれる配信データを前記情報処理端末へ再格納する前に、安全化データ送信要求を前記他の情報処理端末へ送信し、前記情報処理端末の端末固有情報と、前記安全化データ送信要求に対応する第２安全化データに含まれる端末固有情報および流通制御情報とに基づいて、当該第２安全化データに含まれる配信データを前記情報処理端末へ再格納可能か否かを判定し、再格納可能であるときに前記第２安全化データに含まれる前記配信データを前記情報処理端末に格納する、ことを特徴とする。

【００１７】

上述したように、本発明によれば、情報処理端末に格納される配信データは、データ転送を制限する条件を示す流通制御情報をデジタル情報（デジタルコンテンツや電子チケットなどのコンテンツデータ）に付加したものである。流通制御情報としては、たとえば、データ転送の可否決定条件やサーバ問合せの可否決定条件が含まれる。これら条件は、フラグによる記述やプログラムのような手続き的な記述により設定することができる。配信データに含まれるデジタル情報は情報処理端末に格納されてサービス利用者により自由に利用されるが、付加された流通制御情報により当該デジタル情報の転送はサービス提供者の権利が保護されるように制限することができる。これにより、配信データサービス提供者の権利保護とサービス利用者の利便性とを共に確保することができる。

【００１８】

また、他の情報処理端末にバックアップされた安全化データに含まれる配信データをリストアする場合、上述した流通制御情報により、リストアの禁止、無条件リストア許可、および、サーバ問合せのいずれかに設定することができる。サーバ問合せの場合では、サーバは、情報処理端末へリストアする正当性および安全化データの更新の可否を判定し、更新可能であれば、更新された安全化データを返す。これにより、バックアップおよびリストアの正当性を確実に判定するこ

とができる。また、流通制御情報の設定によりサーバに問い合わせる回数を少なくできるために、ネットワークおよびサーバの負荷を軽減できる。

【００１９】

【発明の実施の形態】

１．第１実施形態

図１は、本発明の第１実施形態によるデジタル情報流通制御システムの概略的機能構成を示すブロック図である。本実施形態によるシステムは、サービス提供者サーバ１、通信機能を有する携帯情報端末２、および通信機能を有するユーザ情報端末３を含み、サービス提供者サーバ１と携帯情報端末２およびユーザ情報端末３とがネットワーク４および５によりそれぞれ接続可能であるものとする。

【００２０】

（１）システム構成のアウトライン

サービス提供者サーバ１は、デジタルコンテンツや電子チケットなどのコンテンツデータに流通制御情報を付加し、配信データとしてネットワーク４を通して携帯情報端末２へ送信する。さらに、後述するように、ユーザ情報端末３からの問い合わせに対して更新されたデータを送信する機能も有する。

【００２１】

携帯情報端末２はサービス提供者サーバ１から受信した配信データを格納する。携帯情報端末２はサービス利用者が所有する携帯通信端末や携帯電話機などであり、サービス利用者は、たとえば所定のサービスポイントで電子チケット（入場券など）を利用することができる。さらに、後述するように、携帯情報端末２は配信データのバックアップおよびリストア機能も有する。

【００２２】

ユーザ情報端末３は、ケーブルあるいはワイヤレスにより携帯情報端末２と接続可能であり、携帯情報端末２に格納された配信データのバックアップおよびリストアを行うことができる。後述するように、バックアップされた配信データを携帯情報端末２へリストアする時には、所定の条件に従ってサービス提供者サーバ１へ問い合わせることができる。ユーザ情報端末２としては、ネットワーク５を通してサービス提供者サーバ１に接続可能な通信機能を有するパーソナルコン

ピュータが典型例であるが、その他ネットワーク５に接続されたバックアップ用のコンピュータであってもよい。

【００２３】

図１を参照して更に詳しく説明すると、サービス提供者サーバ１は、コンテンツ・流通制御情報格納部１０１、配信データ管理部１０２、サーバ固有情報格納部１０３および安全化データ更新部１０４を含む。コンテンツ・流通制御情報格納部１０１はデジタルコンテンツや電子チケットなどのコンテンツデータと流通制御情報とを格納する。

【００２４】

流通制御情報は、配信データの流通を制御する情報であり、詳しくは後述するが、携帯情報端末２およびユーザ情報端末３間でのデータ転送の可否、データ転送時の暗号化の要否、あるいは、サービス提供者サーバ１への更新問合せの可否などの少なくとも１つまたは複数について指示する情報である。また、この流通制御情報は、制御フラグまたは手続的記述などにより表現可能である。

【００２５】

配信データ管理部１０２は、コンテンツ・流通制御情報格納部１０１に格納されているコンテンツデータおよび流通制御情報を管理し、それらから生成された配信データを携帯情報端末２へ配信し、あるいは安全化データ更新部１０４へ出力する。なお、コンテンツデータの管理は、外部コンテンツ処理システムと連携して行われる場合もある。たとえば、コンテンツデータが電子チケットの場合には、サービス利用者がサービスを利用する毎に更新される。したがって、その更新内容をコンテンツ・流通制御情報格納部１０１に格納されているコンテンツデータに反映させる必要がある。この場合には、配信データ管理部１０２はネットワーク等を通して外部コンテンツ処理システムに接続されている。

【００２６】

サーバ固有情報格納部１０３は、サービス提供者サーバ１に割り当てられた識別情報やデジタル署名作成および検証のための情報などを含むサーバ固有情報を格納する。

【００２７】

安全化データ更新部１０４は、ユーザ情報端末３から受信した安全化データ更新リクエストに応じた安全化データ更新の可否を判定し、更新可能な場合には安全化データの更新を実行する。なお、安全化データ更新リクエストに応じた安全化データ更新の可否判定は、外部判定システムと連携して行われる。

【００２８】

外部判定システムは、例えば紛失や老朽化などの事由によって携帯情報端末２が機種変更された場合、その変更に伴う端末識別情報などの変更を登録しておき、更新リクエストのコンテンツデータが携帯情報端末２が変更された後でも再発行可能であるか否かを判定する。更新リクエストの端末識別情報が端末変更に起因するものであれば、再発行可能なコンテンツデータであり更新可能であると判定する。更新リクエストの端末識別情報が端末変更と何ら関係がない場合には、更新不可能と判定する。なお、外部判定システムの判定方法は、これに限定されるものではなく、更新リクエストに含まれる情報を利用する他の判定方法でもかまわない。

【００２９】

携帯情報端末２は、配信データ格納部２０１、端末固有情報格納部２０２、安全化データ作成部２０３および安全化データ検証部２０４を有する。配信データ格納部２０１は、サービス提供者サーバ１から受信した配信データあるいは安全化データ検証部２０４から入力したバックアップされた配信データをリストアする。

【００３０】

端末固有情報格納部２０２は、携帯情報端末２に割り当てられた端末識別情報、デジタル署名作成および検証のための情報、コンテンツ暗号化鍵やその証明書情報およびコンテンツ復号化鍵などを含む端末固有情報を格納する。

【００３１】

安全化データ作成部２０３は、配信データ格納部２０１に格納されている配信データと端末固有情報格納部２０２に格納されている端末固有情報とを利用してバックアップ用の安全化データを作成し、ユーザ情報端末３へ送信する。安全化データは、後述するように、そこに含まれるコンテンツデータの不正閲覧を防止

でき、かつ、改ざんの有無を検知することができる。

【００３２】

安全化データ検証部２０４は、バックアップデータのリストアをしようとする時、ユーザ情報端末３へバックアップした安全化データの送信を要求する（安全化データリクエスト）。その要求に応じたユーザ情報端末３から安全化データを受信すると、受信した安全化データに含まれる配信データが保存可能か否かを検証する。保存可能である場合には、受信した配信データを配信データ格納部２０１に格納する。

【００３３】

ユーザ情報端末３は安全化データ格納部３０１および安全化データ更新判定部３０２を有する。安全化データ格納部３０１は、携帯情報端末２から受信したバックアップ用の安全化データを格納する。

【００３４】

安全化データ更新判定部３０２は、携帯情報端末２からの要求に応じて、安全化データ格納部３０１に保存されたバックアップ安全化データに含まれる識別情報や流通制御情報をチェックし、当該安全化データが更新を必要とするか否かを判定する。更新が不要である場合には、携帯情報端末２へ当該安全化データをリストア用の安全化データとして送信する。更新が必要で、かつ、サーバ問合せによる安全化データの更新が許可されている場合には、サービス提供者サーバ１へ当該安全化データを送信して更新を依頼し、サービス提供者サーバ１で更新された安全化データを受信する。そして、サービス提供者サーバ１から受信した安全化データをリストア用の安全化データとして携帯情報端末２へ送信する。

【００３５】

図２は、図１のデジタル情報流通制御システムの全体的なシーケンシャル動作および各端末およびサーバの概略的動作フローを示す流れ図である。

【００３６】

上述したように、本実施形態によるデジタル情報流通制御システムでは、コンテンツデータに流通制御情報が付加された配信データがサービス提供者サーバ１から携帯情報端末２へ配信され、流通制御情報によりデータ転送の可否、データ

転送時の暗号化の要否、サービス提供者サーバ１への更新問合せの可否などが指示される。

【００３７】

図２に示すように、受信した配信データは携帯情報端末２の配信データ格納部２０１に保存され利用に供される。配信データをバックアップする時には、配信データを配信データ格納部２０１から読み出し、端末固有情報格納部２０２に格納された端末固有情報を用いて改ざん等を検知できる安全化データを作成する（ステップＳ０１）。この安全化データをユーザ情報端末３へ送信し、ユーザ情報端末３の安全化データ格納部３０１に格納する（ステップＳ０２）。

【００３８】

バックアップされた配信データをリストアする時には、携帯情報端末２から安全化データリクエストをユーザ情報端末３へ送信する。安全化データ更新判定部３０２は、安全化データリクエストの識別情報とバックアップ安全化データの識別情報および流通制御情報とを用いて、バックアップ安全化データをそのまま返信できるか否か、それともサービス提供者サーバ１への問い合わせが必要か否か、をデータ転送前に判断する（ステップＳ０３）。問い合わせが必要であれば、バックアップ安全化データおよび安全化データリクエストから更新リクエストを生成してサービス提供者サーバ１へ送信する（ステップＳ０４）。

【００３９】

サービス提供者サーバ１は、更新リクエストを受信すると、当該安全化データに含まれるコンテンツデータが改ざんされていない正しい情報であるか否かおよび外部判定システムと連携して更新の可否を判定する（ステップＳ０５）。正しい情報でありかつ更新可と判定されれば、配信データ管理部１０２から最新の配信データを読み出し、更新された安全化データを生成してユーザ情報端末３へ返信する（ステップＳ０６）。なお、サービス提供者は、流通制御情報として予めリストア条件を設定することができるが、コンテンツデータ配信後に利用者が携帯情報端末２の機種変更をしたり、家族が新規に家族割引で契約したりしてもその情報を流通制御情報として与えることはできない。このため、サービス提供者サーバ１にとっても、コンテンツ配信後の携帯情報端末２の機種変更や家族割引

契約情報などは未知の情報である。したがって、機種変更や家族割引契約などに応じてデータ更新可否を制御するためには外部判定システムとの連携が必要である。

【００４０】

サービス提供者サーバ１から更新リクエストに対する更新安全化データを受信すると、安全化データ更新判定部３０２はそれをリストア用の安全化データとして携帯情報端末２へ送信する。また、安全化データ格納部３０１から読み出した安全化データがサーバ問合せを必要としないデータであれば、安全化データ更新判定部３０２はそれをそのままリストア用の安全化データとして携帯情報端末２へ送信する（ステップＳ０３）。

【００４１】

こうして安全化データリクエストの応答としてユーザ情報端末３から安全化データを受信すると、携帯情報端末２の安全化データ検証部２０４は、端末固有情報を参照しながら、受信した安全化データが改ざんされていない正しい情報であるか否か、および、配信データ格納部２０１に格納して良いか否かを判定する（ステップＳ０７）。正しい情報でかつ格納許可された安全化データの配信データのみが配信データ格納部２０１に格納され、配信データのリストアが完了する。

【００４２】

上述した動作により、配信データのバックアップおよびリストアの正当性を確実に判定することができ、利用者の利益とサービス提供者の利益とを両立させることができる。特に、次に説明するようにデジタル署名および暗号化技術を用いてデータ転送および検証を行うことで、より確かな正当性判定およびデータ保護が可能となる。また、流通制御情報の設定によりデータ転送が制御可能であるから、バックアップおよびリストアするための条件を柔軟に設定できる。さらに、流通制御情報の設定により、サーバ１への更新判定問い合わせ、および、更新なしの安全化データリストアを選択することができ、ネットワークおよびサーバの負荷を不必要に増大させることを回避できる。

【００４３】

以下、デジタル情報流通制御システムの具体例を用いて、本実施形態の構成お

よび動作を更に詳細に説明する。

【００４４】

（２）システムの機能構成

図３は、図１に示すデジタル情報流通制御システムのより詳細な機能構成を示すブロック図である。また、図４は携帯情報端末２の端末固有情報格納部２０２に格納される端末固有情報を示す模式図であり、図５はサービス提供者サーバ１のサーバ固有情報格納部１０３に格納されるサーバ固有情報を示す模式図である。

【００４５】

携帯情報端末

配信データ格納部２０１は、サービス提供者サーバ１から配信データを受信する配信データ受信部２２０１と、受信した配信データを記憶する配信データメモリ２２０２と、を有している。

【００４６】

端末固有情報格納部２０２は、図４に示すように、携帯情報端末２とユーザ情報端末３との間を流通する情報に付与するデジタル署名を作成する流通署名作成鍵ｓｋｔと、付与されたデジタル署名を検証する流通署名検証鍵ｖｋｔと、流通署名検証鍵ｖｋｔに対するデジタル証明書である端末証明書ｃ＿ｖｋｔと、コンテンツデータを暗号化するためのコンテンツ暗号化鍵ｅｋと、コンテンツ暗号化鍵ｅｋに対応するコンテンツ復号鍵ｄｋと、コンテンツ暗号化鍵ｅｋに対するデジタル証明書であるコンテンツ暗号化鍵証明書ｃ＿ｅｋと、携帯情報端末あるいは携帯情報端末の所有者を識別するためのＩＤ情報と、を格納している。ＩＤ情報は、たとえば、携帯情報端末毎にユニークに割り当てられた端末識別情報ＩＤｔ、所有者毎にユニークに割り当てられた所有者識別情報ＩＤｕなどである。ただし、ＩＤ情報はこれらに限定されるものではなく、たとえば携帯情報端末や所有者をグループに分類するためのグループＩＤや家族ＩＤなどを含んでもよい。なお、本実施形態におけるＩＤ情報は、端末識別情報ＩＤｔと所有者識別情報ＩＤｕとからなるものとする。

【００４７】

安全化データ作成部２０３は、安全化データ生成部２２０３を有する。安全化データ生成部２２０３は、端末識別情報ＩＤｔ、所有者識別情報ＩＤｕ、配信データ、流通署名Ｓ１、流通署名検証鍵ｖｋｔ、および端末証明書ｃ＿ｖｋｔを含む安全化データを生成する。ここで、流通署名Ｓ１は、配信データと端末識別情報ＩＤｔおよび所有者識別情報ＩＤｕとを含む情報に対して流通署名作成鍵ｓｋｔを用いたデジタル署名処理を実行することにより生成される。なお、後述するように、配信データに含まれるコンテンツデータをコンテンツ暗号化鍵ｅｋを用いて暗号化したものを用いて、安全化データを生成してもよい。こうして生成された安全化データは、送受信部２２０７を通してユーザ情報端末３へ送信される。

【００４８】

安全化データ検証部２０４は、安全化データリクエスト生成部２２０４と、流通署名検証鍵検証部２２０５およびデータ安全性確認部２２０６と、を有する。

【００４９】

安全化データリクエスト生成部２２０４は、ユーザ情報端末３に保存されている安全化データを要求するために、端末識別情報ＩＤｔおよび所有者識別情報ＩＤｕを含む安全化データリクエスト、あるいは、端末識別情報ＩＤｔ、所有者識別情報ＩＤｕ、コンテンツ暗号化鍵ｅｋおよびコンテンツ暗号化鍵証明書ｃ＿ｅｋを含む安全化データリクエストを生成する。生成された安全化データリクエストは送受信部２２０７を通してユーザ情報端末３へ送信される。

【００５０】

安全化データリクエストの応答として安全化データが送受信部２２０７を通してユーザ情報端末３から受信されると、その安全化データは、サービス提供者サーバ１で更新されたものか、あるいは、携帯情報端末２で生成されユーザ情報端末３にバックアップされたものかのいずれかである。

【００５１】

流通署名検証鍵検証部２２０５は、受信した安全化データに含まれる端末証明書ｃ＿ｖｋｔあるいはサービス提供者証明書ｃ＿ｖｋｓ（図５参照）を利用して、当該安全化データに含まれる流通署名検証鍵ｖｋｔあるいはｖｋｓが正しいこ

とを検証する。

【００５２】

データ安全性確認部２２０６は、流通署名検証鍵が検証された安全化データに付与されている流通署名を利用して、当該安全化データが改ざんされていない正しいデータであることを確認すると共に、当該安全化データが携帯情報端末２で生成したものか、サービス提供者サーバ１で生成されたものかを判定する。さらに、当該安全化データに含まれる配信データを配信データメモリ２２０２へ保存してよいか否かを判定する。保存可能と判定された場合には配信データメモリ２２０２へ保存する。もし安全化データに含まれるコンテンツデータが暗号化されていれば、コンテンツ復号鍵によって復号してから保存する。

【００５３】

ユーザ情報端末

ユーザ情報端末３は携帯情報端末２との間でデータのやりとりを行うための送受信部２３０１を有し、安全化データ格納部３０１は受信した安全化データを記憶する安全化データメモリ２３０２を有する。

【００５４】

安全化データ更新判定部３０２は、更新要否判定部２３０３、更新リクエスト生成部２３０４、および、送受信部２３０５を有する。

【００５５】

送受信部２３０１により携帯情報端末２から安全化データリクエストを受信すると、更新要否判定部２３０３は、安全化データメモリ２３０２に記憶されているバックアップ安全化データに含まれる流通制御情報と、受信した安全化データリクエストに含まれる端末識別情報ＩＤｔあるいは所有者識別情報ＩＤｕとを比較し、当該バックアップ安全化データの更新の要否を判定する。

【００５６】

更新要否判定部２３０３によって更新不要と判定された場合には、当該バックアップ安全化データは送受信部２３０１を通してそのまま携帯情報端末２へ送信される。更新要否判定部２３０３により更新が必要と判定された場合には、更新リクエスト生成部２３０４はバックアップ安全化データと安全化データリクエス

トとを含む更新リクエストを生成し、送受信部２３０５を通してサービス提供者サーバ１へ送信する。

【００５７】

この更新リクエストに対する応答として、サービス提供者サーバ１から更新済みの安全化データを送受信部２３０５で受信すると、当該更新済み安全化データは送受信部２３０１を通して携帯情報端末２へ送信される。更新済み安全化データを受信した携帯情報端末２では、上述したように、流通署名検証鍵検証部２２０５およびデータ安全性確認部２２０６により更新済み安全化データの正当性および安全性が確認された後、配信データメモリ２２０２に格納される。

【００５８】

サービス提供者サーバ

コンテンツ／流通制御情報格納部１０１は、サービス利用者に配信するデジタルコンテンツや電子チケット等のコンテンツデータを記憶するコンテンツメモリ２１０１と、コンテンツデータの各々に対応する流通制御情報を記憶する流通制御情報メモリ２１０２とを含む。なお、上述したように、コンテンツメモリ２１０１のコンテンツデータによっては、外部コンテンツ処理システム２４０１によりその内容が更新されるものもある。

【００５９】

配信データ管理部１０２は、コンテンツメモリ２１０１に記憶されているコンテンツデータとそれに対応する流通制御情報とから配信データを生成する配信データ生成部２１０３と、配信データを携帯情報端末２へ配信する配信データ配信部２１０４とを有している。

【００６０】

サーバ固有情報格納部１０３は、図５に示すように、サービス提供者の識別情報ＩＤｓと、携帯情報端末２、ユーザ情報端末３およびサービス提供者サーバ１の間を流通する情報に付与するデジタル署名を作成するための流通署名作成鍵ｓｋｓと、付与されたデジタル署名を検証するための流通署名検証鍵ｖｋｓと、流通署名検証鍵に対するデジタル証明書であるサービス提供者証明書ｃ＿ｖｋｓと、を格納している。

【００６１】

安全化データ更新部１０４は、送受信部２１０５、流通署名検証鍵検証部２１０６、更新可否判定部２１０７、コンテンツ暗号化鍵検証部２１０８、および、安全化データ更改部２１０９を有する。

【００６２】

送受信部２１０５によりユーザ情報端末３から更新リクエストを受信すると、流通署名検証鍵検証部２１０６は、更新リクエストに含まれる端末証明書ｃ＿ｖｋｔを利用して当該更新リクエストに含まれる流通署名検証鍵ｖｋｔが正しいことを検証する。続いて、更新可否判定部２１０７は、検証された流通署名検証鍵を用いて、当該更新リクエストに含まれる安全化データが改ざんされていない正しい情報であることを検証し、さらに、外部判定システム２４０２においてサービス提供者が決定する更新要件を参照し、更新リクエストに含まれる安全化データの更新可否を判定する。更新可能であれば、コンテンツ暗号化鍵検証部２１０８は、更新リクエストに含まれるコンテンツ暗号化鍵証明書ｃ＿ｅｋを用いて更新リクエストに含まれるコンテンツ暗号化鍵ｅｋが正しいことを検証する。

【００６３】

コンテンツ暗号化鍵ｅｋの正当性が検証されると、安全化データ更改部２１０９は、更新リクエストに含まれる安全化データを参照して、配信データ生成部２１０３から対応する配信データを取得し、サーバ固有情報格納部１０３に格納されているサービス提供者識別情報ＩＤｓ、流通署名作成鍵ｓｋｓ、流通署名検証鍵ｖｋｓおよびサービス提供者証明書ｃ＿ｖｋｓを用いて更新安全化データを生成する。その際、正しいことが確認されたコンテンツ暗号化鍵ｅｋを用いてコンテンツデータを暗号化して更新安全化データを生成してもよい。こうして得られた更新安全化データは、更新リクエストの応答として、送受信部２１０５を通してユーザ情報端末３へ返信される。

【００６４】

（３）動作例

まず、本発明によるデジタル情報流通制御システムでは、システム管理者がサービス提供者に対して

●サービス提供者サーバ毎に異なるサービス提供者識別情報の割り当ておよび発行
●サービス提供者証明書の発行
を実施する。

【００６５】

サービス提供者は、発行されたサービス提供者識別情報およびサービス提供者証明書、サービス提供者自身が作成したデータであることを証明するデジタル署名を作成するための流通署名作成鍵、および流通署名作成鍵に対応する流通署名検証鍵を管理する。特に流通署名作成鍵は他者に知られることのないように安全に管理する。ここで、流通署名作成鍵および流通署名検証鍵の作成は、サービス提供者によって実施されてもよく、この場合、システム管理者は、サービス提供者が示した流通署名検証鍵に対するサービス提供者証明書を発行すればよい。

【００６６】

また、システム管理者は、サービス利用者が所有する携帯情報端末２に対して、
●携帯情報端末毎に異なる端末識別情報の割り当ておよび各携帯情報端末への転送
●サービス利用者毎に異なる所有者識別情報の割り当ておよび各携帯情報端末への　転送
●流通署名作成鍵およびそれに対応する流通署名検証鍵の作成と各携帯情報端末へ　の転送
●端末証明書の作成および各携帯情報端末への転送
●コンテンツ暗号化鍵の各携帯情報端末への転送
●コンテンツ暗号化鍵に対応するコンテンツ復号鍵の生成および各携帯情報端末へ　の転送
を実施する。

【００６７】

特に、流通署名作成鍵およびコンテンツ復号鍵は携帯情報端末内の耐タンパ性(tamper-resistant)のあるストレージなどに格納し、悪意のユーザによる入手を

困難にしておく。ここで、コンテンツ暗号化鍵は、システム管理者が作成して発行し携帯情報端末へ転送してもよいし、サービス利用者によって作成され、システム管理者に示したものを携帯情報端末へ転送してもよい。

【００６８】

また、コンテンツ暗号化鍵／コンテンツ復号鍵は公開鍵暗号系の暗号化鍵／復号鍵のペアであり、コンテンツ暗号化鍵で暗号化した情報は、対応するコンテンツ復号鍵でのみ復号でき、コンテンツ暗号鍵からコンテンツ復号化鍵を生成するための落とし戸関数を知らなければコンテンツ暗号化鍵からコンテンツ復号鍵を生成することは十分に困難であるものとする。尚、落とし戸関数はシステム管理者により十分安全に管理されているものとする。

【００６９】

次に、携帯情報端末２の端末固有情報格納部２０２は図４に示す端末固有情報を格納し、サービス提供者サーバ１のサーバ固有情報格納部１０３は図５に示すサーバ固有情報を格納しているものとし、本実施形態におけるデータ配信、バックアップおよびリストア動作の具体例を詳細に説明する。

【００７０】

<u>データ配信</u>

図６（Ａ）は配信データ生成部２１０３で生成される配信データの構成の一例を示す模式図であり、（Ｂ）はその流通制御情報の記述例を示す模式図である。

【００７１】

図６（Ａ）に示すように、配信データは管理用ヘッダ（Ｈ）、コンテンツボディ（Ｂ）および流通制御情報（Ｐ）から構成される。管理用ヘッダ（Ｈ）は携帯情報端末２へ配信するコンテンツデータを個別に管理するための情報であり、サービス提供者名やコンテンツデータのシリアル番号などを含んでいる。コンテンツボディ（Ｂ）は携帯情報端末２へ配信するデジタルコンテンツや電子チケットなどのコンテンツデータそのものである。

【００７２】

流通制御情報（Ｐ）は携帯情報端末２へ配信した配信データの流通を制御する情報である。たとえば、流通制御情報を含むデータを格納した情報端末からバッ

クアップ用情報端末へデータを転送して格納しているものとする。そのバックアップデータをバックアップ用情報端末からある情報端末へリストアする際に、リストアを要求している情報端末とバックアップデータが示す情報端末との同一性、および、バックアップデータに含まれる流通制御情報が示す条件に基づいて、転送許可／サーバ問い合わせ／転送禁止が決定される。例えば、

・　「バックアップしたデータに含まれる端末識別情報と、リストア先の情報端末が持つ端末識別情報とが一致した場合にはリストア許可」、

・　「バックアップしたデータに含まれる所有者識別情報と、リストア先の情報端末が持つ所有者識別情報とが一致しない場合には、サービス提供者サーバ１へ問合せ、その後リストア許可」、

・　「バックアップしたデータに含まれる端末識別情報と、リストア先の情報端末が持つ端末識別情報とが一致しない場合にはリストア不許可」

のような制御が可能となる。

【００７３】

図６（Ｂ）に示すように、ここでは、４つのフラグで記述された流通制御情報が一例として示されている。最初のフラグは同一端末間移動フラグＦｔで、禁止／許可／サービス提供者サーバ問合せの３値をとる。次のフラグは同一所有者間移動フラグF_{u1}で、禁止／許可／サービス提供者サーバ問合せの３値をとる。次のフラグは異所有者間移動フラグF_{u2}で、禁止／許可／サービス提供者サーバ問合せの３値をとる。次のフラグは暗号化フラグF_{en}でコンテンツボディの暗号化を行わない／行うの２値をとる。

【００７４】

図６（Ｂ）に示した例は流通制御情報の一例であり、それぞれのフラグは異なる順番でもよい。また、流通制御情報内に、端末識別情報や所有者識別情報を固定的に埋め込んでおき、埋め込まれた端末識別情報や所有者識別情報と、安全化データの転送を要求する携帯情報端末２の端末識別情報や所有者識別情報との一致／不一致を条件として記述してもよい。さらに、端末識別情報や所有者識別情報が番号として記述される場合には、その大小関係を条件としてもよい。あるいは、後述するように、流通制御情報（Ｐ）をプログラムで手続き的に記述しても

よい（図２３参照）。

【００７５】

なお、配信データの管理用ヘッダおよびコンテンツボディはコンテンツメモリ２１０１に記憶されており、流通制御情報は流通制御情報メモリ２１０２に記憶されている。

【００７６】

配信データ生成部２１０３で生成された配信データは、配信データ配信部２１０４から携帯情報端末２へ配信され、携帯情報端末２において配信データ受信部２２０１で受信されて配信データメモリ２２０２に格納される。格納された配信データは、配信データ生成部２１０３で生成した配信データと同様であり、図６に示す情報を含んでいる。

【００７７】

ここで、配信データ配信部２１０４と配信データ受信部２２０１との間の通信がインターネットや公衆網を用いる場合には、通信経路での配信データ内に含まれるコンテンツデータの盗聴を防止するための暗号化通信が望ましい。このような暗号化通信は、ＳＳＬ（セキュア・ソケット・レイヤー）暗号化通信など、広く一般的に知られている技術で実現することが可能である。また、携帯情報端末２へ配信された配信データを悪意のユーザによる盗用から保護するためには、配信データメモリ２２０２は本発明によるシステム以外からはアクセスできないこと、あるいは、暗号化により実質的にアクセスできないことが重要である。

【００７８】

バックアップ

図７（Ａ）は、安全化データ生成部２２０３で生成され、送信時にコンテンツボディの暗号化を行わないと指定されたバックアップ用安全化データの構成例を示す模式図であり、（Ｂ）は、安全化データ生成部２２０３で生成され、送信時にコンテンツボディの暗号化を行うと指定されたバックアップ用安全化データの構成例を示す模式図である。

【００７９】

図７（Ａ）に示す安全化データ７０１は、携帯情報端末２に格納されている端

末識別情報（ＩＤｔ）、所有者識別情報（ＩＤｕ）、配信データに含まれる管理用ヘッダ（Ｈ）、コンテンツボディ（Ｂ）および流通制御情報（Ｐ）、流通署名（Ｓ１）、流通署名検証鍵（ｖｋｔ）、および端末証明書（ｃ＿ｖｋｔ）を含んでいる。流通署名（Ｓ１）は、端末識別情報（ＩＤｔ）、所有者識別情報（ＩＤｕ）、管理用ヘッダ（Ｈ）、コンテンツボディ（Ｂ）、および、流通制御情報（Ｐ）を結合したデータに対して、携帯情報端末２に格納されている流通署名作成鍵（ｓｋｔ）を用いて作成したデジタル署名である：Ｓ1 = Sig[skt(IDt+IDu+H+B+P)]。

【００８０】

図７（Ｂ）に示す安全化データ７０２は、送信時にコンテンツボディの暗号化を行うと指定された場合の安全化データであり、携帯情報端末２に格納されている端末識別情報（ＩＤｔ）、所有者識別情報（ＩＤｕ）、配信データに含まれる管理用ヘッダ（Ｈ）、コンテンツボディ（Ｂ）を暗号化した暗号化コンテンツボディ（Ｅ）および流通制御情報（Ｐ）、流通署名（Ｓ２）、流通署名検証鍵（ｖｋｔ）、および端末証明書（ｃ＿ｖｋｔ）を含んでいる。ここで、暗号化コンテンツボディ（Ｅ）は、携帯情報端末２に格納されているコンテンツ暗号化鍵（ｅｋ）を用いて作成する。また、流通署名（Ｓ２）は、端末識別情報（ＩＤｔ）、所有者識別情報（ＩＤｕ）、管理用ヘッダ（Ｈ）、暗号化コンテンツボディ（Ｅ）、および、流通制御情報（Ｐ）を結合したデータに対して、携帯情報端末２に格納されている流通署名作成鍵（ｓｋｔ）を用いて作成したデジタル署名である：Ｓ2 = Sig[skt(IDt+IDu+H+E+P)]。

【００８１】

このようにして生成されたバックアップ用安全化データ７０１または７０２は送受信部２２０７を通してユーザ情報端末３へ送信される。

【００８２】

ユーザ情報端末３において、送受信部２３０１は携帯情報端末２からバックアップ用安全化データを受信し、安全化データメモリ２３０２に記憶する。安全化データメモリ２３０２に記憶されるデータは、図７に示した安全化データを少なくとも含んでいればよく、それ以外の情報を併せて格納することも可能である。

たとえば、保存日時情報を合わせて記憶しておけば、最後に転送した安全化データであることを識別することができる。

【００８３】

リストア

次に、ユーザ情報端末３に格納した安全化データを携帯情報端末２へ復元する動作について説明する。

【００８４】

１）安全化データリクエスト

図８は安全化データリクエスト生成部２２０４で生成する安全化データリクエストの構成例を示す模式図である。図８において安全化データリクエストは端末識別情報（ＩＤｔ’）、所有者識別情報（ＩＤｕ’）、コンテンツ暗号化鍵（ｅｋ’）、コンテンツ暗号化鍵証明書（ｃ＿ｅｋ’）を含んで構成される。ここで記号「’」（ダッシュ）は、安全化データリクエストを生成する携帯情報端末の端末固有情報を、先に安全化データを作成した携帯情報端末の端末固有情報から区別するために付加したものである。すなわち、同一の携帯情報端末であれば端末固有情報は完全に一致するが、正当にあるいは不正に異なる携帯情報端末を用いて安全化データリクエストを生成した場合には、これら端末固有情報が一致しないことを考慮したものである。

【００８５】

安全化データリクエストには、図８に示した情報の他に、リクエストする安全化データを識別するための情報を含んでもよい。また、安全化データを識別する情報が含まれない場合には、ユーザ情報端末３で保存している安全化データを全てリクエストしたものと解釈する。あるいは、ユーザ情報端末３がユーザインタフェースを持つ場合には、それをユーザに操作させ、携帯情報端末２へ転送したい安全化データを選択してもよい。

【００８６】

安全化データリクエスト生成部２２０４で生成した安全化データリクエストは、送受信部２２０７を通して携帯情報端末２からユーザ情報端末３へ送信される。ユーザ情報端末３は、送受信部２３０１で安全化データリクエストを受信し、

更新要否判定部２３０３へ転送する。

【００８７】

２）更新要否判定

更新要否判定部２３０３は、安全化データメモリ２３０２に記憶されているバックアップ安全化データを読み出し、バックアップ安全化データに含まれる流通制御情報と、安全化データリクエストに含まれる端末識別情報および所有者識別情報とを比較する。この比較結果に応じて、バックアップ安全化データをそのまま携帯情報端末２へ転送するか、あるいは、サービス提供者サーバ１に転送判定および安全化データの更新要求を依頼するか否かを判定する。

【００８８】

図９は更新要否判定部２３０３の安全化データ更新判定動作の一例を示すフローチャートである。ここでは、ＩＤ情報が端末識別情報ＩＤｔおよび所有者識別情報ＩＤｕからなり、さらに安全化データが図６（Ｂ）に示した流通制御情報を含んでいる場合を例示する。ＩＤ情報がグループＩＤあるいは家族ＩＤなどからなる場合も同様である。

【００８９】

図９において、更新要否判定部２３０３は、まずバックアップ安全化データに含まれる端末識別情報（ＩＤｔ）と安全化データリクエストに含まれる端末識別情報（ＩＤｔ’）とを比較する（ステップＳ１）。

【００９０】

ＩＤｔ＝ＩＤｔ’であれば（ステップＳ１のＹＥＳ）、続いてバックアップ安全化データに含まれる流通制御情報の同一端末間移動フラグ（Ｆｔ）の値が「１：許可」であるか否かを判定する（ステップＳ２）。Ｆｔ＝１（同一端末間移動許可）であれば（ステップＳ２のＹＥＳ）、バックアップ安全化データを送受信部２３０１を通してそのまま携帯情報端末２へ転送する（転送許可）。

【００９１】

Ｆｔ≠１であれば（ステップＳ２のＮＯ）、更新要否判定部２３０３は、さらに、バックアップ安全化データに含まれる流通制御情報の同一端末間移動フラグ（Ｆｔ）の値が「２：サービス提供者サーバ問合せ」であるかを判定する（ステ

ップＳ３）。Ｆｔ＝２であれば（ステップＳ３のＹＥＳ）、更新要否判定部２３０３は更新リクエスト生成部２３０４へバックアップ安全化データを転送し、後述するサーバ問合せ処理を開始する。Ｆｔ≠２であれば（ステップＳ３のＮＯ）、Ｆｔ＝０（転送禁止）と判断され、携帯情報端末２へのリストアは禁止される。

【００９２】

一方、ＩＤｔ≠ＩＤｔ’であれば（ステップＳ１のＮＯ）、更新要否判定部２３０３は、バックアップ安全化データに含まれる所有者識別情報（ＩＤｕ）と安全化データリクエストに含まれる所有者識別情報（ＩＤｕ’）を比較する（ステップＳ４）。

【００９３】

ＩＤｕ＝ＩＤｕ’であれば（ステップＳ４のＹＥＳ）、続いてバックアップ安全化データに含まれる流通制御情報の同一所有者間移動フラグ（F_{ul}）の値が「１：許可」であるか否かを判定する（ステップＳ５）。F_{ul}＝１（同一所有者間移動許可）であれば（ステップＳ５のＹＥＳ）、バックアップ安全化データを送受信部２３０１を通してそのまま携帯情報端末２へ転送する（転送許可）。

【００９４】

F_{ul}≠１であれば（ステップＳ５のＮＯ）、更新要否判定部２３０３は、さらに、バックアップ安全化データに含まれる流通制御情報の同一所有者間移動フラグ（F_{ul}）の値が「２：サービス提供者サーバ問合せ」であるかを判定する（ステップＳ６）。F_{ul}＝２であれば（ステップＳ６のＹＥＳ）、更新要否判定部２３０３は更新リクエスト生成部２３０４へバックアップ安全化データを転送し、後述するサーバ問合せ処理を開始する。F_{ul}≠２であれば（ステップＳ６のＮＯ）、F_{ul}＝０（転送禁止）と判断され、携帯情報端末２へのリストアは禁止される。

【００９５】

ＩＤｕ≠ＩＤｕ’であれば（ステップＳ４のＮＯ）、更新要否判定部２３０３は、バックアップ安全化データに含まれる流通制御情報の異ユーザ者間移動フラグ（F_{u2}）の値が「１：許可」であるか否かを判定する（ステップＳ７）。F_{u2}

＝１（異ユーザ間移動許可）であれば（ステップＳ７のＹＥＳ）、バックアップ安全化データを送受信部２３０１を通してそのまま携帯情報端末２へ転送する（転送許可）。

【００９６】

F_{u2}≠１であれば（ステップＳ７のＮＯ）、更新要否判定部２３０３は、さらに、異ユーザ者間移動フラグ（F_{u2}）の値が「２：サービス提供者サーバ問合せ」であるかを判定する（ステップＳ８）。F_{u2}＝２であれば（ステップＳ８のＹＥＳ）、更新要否判定部２３０３は更新リクエスト生成部２３０４へバックアップ安全化データを転送し、後述するサーバ問合せ処理を開始する。F_{u2}≠２であれば（ステップＳ８のＮＯ）、F_{u2}＝０（転送禁止）と判断され、携帯情報端末２へのリストアは禁止される。

【００９７】

このように、バックアップ安全化データを携帯情報端末２へ転送するか（転送許可）、サービス提供者サーバに転送判定および安全化データの更新を依頼するか（サーバ問合せ）、あるいは、転送しないか（転送禁止）を判定することができる。ただし、判定方法はこれに限定されるものではない。流通制御情報に記録されている情報と安全化データリクエストに含まれる情報とを利用し、転送許可／サーバ問合せ／転送禁止が判定できれば他の判定方法でもよい。なお、流通制御情報は、後述するように手続的に記述される場合もある。

【００９８】

３）サーバ問合せ

更新要否判定部２３０３が「サーバ問合せ」と判定した場合、更新リクエスト生成部２３０４は更新リクエストを生成する。

【００９９】

図１０は更新リクエストの構成例を示す模式図である。更新リクエストは、少なくともバックアップ安全化データと安全化データリクエストとを含んでいる。なお、図１０に示す更新リクエストでは、暗号化されていないコンテンツボディ（Ｂ）の場合と暗号化コンテンツボディ（Ｅ）の場合とが記載されている。送受信部２３０５は生成された更新リクエストをサービス提供者サーバ１へ送信する

。

【０１００】

サービス提供者サーバ１において、ユーザ情報端末３から更新リクエストを受信すると、流通署名検証鍵検証部２１０６は更新リクエストに含まれる端末証明書（ｃ＿ｖｋｔ）を元に、流通署名検証鍵（ｖｋｔ）がシステム管理者により割り当てられた正当な流通署名検証鍵であることを検証する。ただし、流通署名検証鍵検証部２１０６は端末証明書の正しさを検証するために必要な情報を保持しているものとする。

【０１０１】

流通署名検証鍵（ｖｋｔ）の正当性が否定された場合、サーバ問合せによる安全化データの更新は失敗し、携帯情報端末２への安全化データ転送の処理（リストア）は中止する。

【０１０２】

流通署名検証鍵（ｖｋｔ）の正当性が検証された場合、更新可否判定部２１０７は、更新リクエストに含まれる流通署名検証鍵（ｖｋｔ）によって、流通署名Ｓ１あるいは流通署名Ｓ２に基づいて端末識別情報（ＩＤｔ）、所有者識別情報（ＩＤｕ）、管理用ヘッダ（Ｈ）、コンテンツボディ（Ｂ）または暗号化コンテンツボディ（Ｅ）、および、流通制御情報（Ｐ）が改ざんされていない正しい情報であることを検証する。さらに、端末識別情報（ＩＤｔ、ＩＤｔ’）、所有者識別情報（ＩＤｕ、ＩＤｕ’）、管理用ヘッダ（Ｈ）を元に、外部判定システム２４０２と連携して、バックアップ安全化データに含まれているコンテンツデータを端末識別情報ＩＤｔ’の携帯情報端末へ転送して復元してよいか否かを判定する。バックアップ安全化データおよび転送先の携帯情報端末の正当性が確認されると、バックアップ安全化データの更新可能と判定される。

【０１０３】

バックアップ安全化データの更新が可能と決定された場合、コンテンツ暗号化鍵検証部２１０８は、更新リクエストに含まれるコンテンツ暗号化鍵証明書（ｃ＿ｅｋ’）を元に、コンテンツ暗号化鍵（ｅｋ’）がシステム管理者により正しく割り当てられたコンテンツ暗号化鍵であることを検証する。なお、コンテンツ

暗号化鍵検証部２１０８はコンテンツ暗号化鍵証明書の正しさを検証するために必要な情報を保持しているものとする。コンテンツ暗号化鍵（ｅｋ’）の検証に失敗した場合は、サーバ問合せによる安全化データの更新は失敗し、携帯情報端末２への安全化データ転送の処理は中止する。

【０１０４】

コンテンツ暗号化鍵（ｅｋ’）の検証に成功した場合、安全化データ更改部２１０９は、配信データ生成部２１０３から配信データを取得して更新された安全化データを生成する。

【０１０５】

図１１（Ａ）は、安全化データ更改部２１０９で生成され、送信時にコンテンツボディの暗号化を行わないと指定された更新安全化データの構成例を示す模式図であり、（Ｂ）は、安全化データ更改部２１０９で生成され、送信時にコンテンツボディの暗号化を行うと指定された更新安全化データの構成例を示す模式図である。

【０１０６】

図１１（Ａ）に示す安全化データ１１０１は、サービス提供者によって更新された安全化データであることを示すサービス提供者更新フラグ（Ｆ）、サービス提供者サーバに格納されているサービス提供者識別情報（ＩＤｓ）、配信データ生成部２１０３で改めて生成された配信データ（Ｈ”、Ｂ”およびＰ”）、流通署名検証鍵（ｖｋｓ）、サービス提供者証明書（ｃ＿ｖｋｓ）、および、流通署名（Ｓ１”）を含んでいる。

【０１０７】

流通署名（Ｓ１”）は、サーバ固有情報格納部１０３に格納されている流通署名作成鍵（ｓｋｓ）を用いて作成されるデジタル署名である。具体的には、配信データ生成部２１０３で改めて生成した配信データに含まれる管理用ヘッダ（Ｈ”）、コンテンツボディ（Ｂ”）および流通制御情報（Ｐ”）と、更新リクエストに含まれている端末識別情報（ＩＤｔ’）と、サービス提供者更新フラグ（Ｆ）と、サービス提供者識別情報（ＩＤｓ）と、を結合したデータに対して、流通署名作成鍵（ｓｋｓ）を用いて作成される：　Sl” =　Sig[skt(F + IDs + IDt’ +

H" + B" + P")]。

【０１０８】

図１１（Ｂ）に示す安全化データ１１０２は、サービス提供者によって更新された安全化データであることを示すサービス提供者更新フラグ（Ｆ）、サービス提供者サーバに格納されているサービス提供者識別情報（ＩＤｓ）、配信データ生成部２１０３で改めて生成された配信データ（H"、E"およびP"）、流通署名検証鍵（ｖｋｓ）、サービス提供者証明書（ｃ＿ｖｋｓ）、および、流通署名（Ｓ２"）を含んでいる。

【０１０９】

流通署名（Ｓ２"）は、サーバ固有情報格納部１０３に格納されている流通署名作成鍵（ｓｋｓ）を用いて作成されるデジタル署名である。具体的には、配信データ生成部２１０３で改めて生成した配信データに含まれる管理用ヘッダ（H"）、コンテンツボディ（B"）を暗号化した暗号化コンテンツボディ（E"）および流通制御情報（P"）と、更新リクエストに含まれている端末識別情報（ＩＤｔ'）と、サービス提供者更新フラグ（Ｆ）と、サービス提供者識別情報（ＩＤｓ）と、を結合したデータに対して、流通署名作成鍵（ｓｋｓ）を用いて作成される：S2" = Sig[skt(F + IDs + IDt' + H" + E" + P")]。なお、暗号化コンテンツボディは更新リクエストに含まれていて、検証されたコンテンツ暗号化鍵（ｅｋ'）を用いて作成する。

【０１１０】

ここで、記号「"」（ツーダッシュ）は、更新リクエストに含まれている配信データの管理用ヘッダ（Ｈ）、コンテンツボディ（Ｂ）／暗号化コンテンツボディ（Ｅ）、および、流通制御情報（Ｐ）と区別するためにつけたものである。上述したように、コンテンツメモリ２１０１に記憶されているコンテンツデータは外部コンテンツ処理システム２４０１によって更新される場合があり、サービス提供者サーバ１から携帯情報端末２に配信した配信データとは異なる場合があることを意味している。もちろん外部コンテンツ処理システム２４０１による更新はなく、同一の配信データであってもよい。

【０１１１】

このようにして更新された安全化データは送受信部２１０５を介してユーザ情報端末３へ送信される。更新された安全化データを受信すると、ユーザ情報端末３は当該更新安全化データをリストア用安全化データとして携帯情報端末２へ送信する。

【０１１２】

４）安全性確認およびリストア

携帯情報端末２において送受信部２２０７は、ユーザ情報端末３から安全化データを受信する。この受信した安全化データは、サービス提供者サーバ１による更新がない場合には図７に示すような安全化データ７０１または７０２であり、サービス提供者サーバ１による更新があった場合には図１１に示すような安全化データ１１０１または１１０２である。

【０１１３】

流通署名検証鍵検証部２２０５は、受信した安全化データに含まれる端末証明書（ｃ＿ｖｋｔ）を元に、流通署名検証鍵（ｖｋｔ）がシステム管理者により正しく割り当てられた流通署名検証鍵であることを検証する。あるいは、受信した安全化データに含まれるサービス提供者証明書（ｃ＿ｖｋｓ）を元に、流通署名検証鍵（ｖｋｓ）が、システム管理者により正しく割り当てられた流通署名検証鍵であることを検証する。なお、流通署名検証鍵検証部２２０５は端末証明書及びサービス提供者証明書の正しさを検証するために必要な情報を保持しているものとする。

【０１１４】

データ安全性確認部２２０６では、流通署名検証鍵検証部２２０５で検証された流通署名検証鍵（ｖｋｔまたはｖｋｓ）を用いて、安全化データに含まれる流通署名（Ｓ１／Ｓ２またはＳ１”／Ｓ２”）を元に、受信した安全化データが改ざんされていないことを確認する。改ざんが検知されたら処理を中断する。改ざんされていない場合には、次に説明するデータ安全性確認が行われる。

【０１１５】

図１２はデータ安全性確認部２２０６におけるデータ安全性確認動作の一例を示すフローチャートである。ここでは、ＩＤ情報が端末識別情報ＩＤｔおよび所

有者識別情報ＩＤｕからなり、さらに安全化データが図６（Ｂ）に示した流通制御情報を含んでいる場合を例示する。ＩＤ情報がグループＩＤあるいは家族ＩＤなどからなる場合も同様である。

【０１１６】

図１２において、データ安全性確認部２２０６は正当性が確認された安全化データにサービス提供者更新フラグ（Ｆ）が含まれるか否かを判定する（ステップＳ１１）。サービス提供者更新フラグ（Ｆ）が含まれる場合は（ステップＳ１１のＹＥＳ）、サービス提供者サーバ１による更新があると判断され、安全化データに含まれる端末識別情報（ＩＤｔ’）と携帯情報端末２に記憶されている端末識別情報（ＩＤｔ”）とを比較する（ステップＳ１２）。

【０１１７】

ＩＤｔ’＝ＩＤｔ”であれば（ステップＳ１２のＹＥＳ）、同一の携帯情報端末であるから、正当性が確認された安全化データに含まれる配信データ（Ｈ”、Ｂ”、Ｐ”）を復元し、配信データメモリ２２０２に格納する（格納許可）。なお、正当性が確認された安全化データに暗号化コンテンツボディ（Ｅ”）が含まれている場合には、コンテンツ復号鍵（ｄｋ”）を用いて復号し、管理用ヘッダ（Ｈ”）、コンテンツボディ（Ｂ”）および流通制御情報（Ｐ”）からなる配信データを復元し、配信データメモリ２２０２へ格納する。ここで、暗号化コンテンツボディを正しく復号するためには、コンテンツ復号鍵（ｄｋ’）とコンテンツ復号鍵（ｄｋ”）が一致している必要がある。コンテンツ復号鍵の一致は、サービス利用者がコンテンツ暗号化鍵を管理し、システム管理者が生成して携帯情報端末へ格納するコンテンツ復号鍵を間接的に管理するか、サービス提供者が配信データに含まれる流通制御情報を工夫することで実現できる。

【０１１８】

ＩＤｔ’≠ＩＤｔ”であれば（ステップＳ１２のＮＯ）、配信データメモリ２２０２への格納は禁止される（格納禁止）。

【０１１９】

また、サービス提供者更新フラグ（Ｆ）が含まれていない場合は（ステップＳ１１のＮＯ）、サービス提供者サーバ１による更新がないと判断され、安全化デ

ータに含まれる端末識別情報（ＩＤｔ）と携帯情報端末に記憶されている端末識別情報（ＩＤｔ”）とを比較する（ステップＳ１３）。ＩＤｔ＝ＩＤｔ”であれば（ステップＳ１３のＹＥＳ）、さらに、安全化データに含まれる流通制御情報の同一端末間移動フラグ（Ｆｔ）の値が「１：許可」であるか否かを判定する（ステップＳ１４）。Ｆｔ＝１であれば（ステップＳ１４のＹＥＳ）、上述したように配信データメモリ２２０２への格納が許可される（格納許可）。なお、正当性が確認された安全化データに暗号化コンテンツボディ（Ｅ）が含まれている場合には、コンテンツ復号鍵（ｄｋ）を用いて復号し、管理用ヘッダ（Ｈ）、コンテンツボディ（Ｂ）および流通制御情報（Ｐ）からなる配信データを復元し、配信データメモリ２２０２へ格納する。ここで、暗号化コンテンツボディを正しく復号するためには、コンテンツ復号鍵（ｄｋ）とコンテンツ復号鍵（ｄｋ”）が一致している必要がある。コンテンツ復号鍵の一致は、サービス利用者がコンテンツ暗号化鍵を管理し、システム管理者が生成して携帯情報端末へ格納するコンテンツ復号鍵を間接的に管理するか、サービス提供者が配信データに含まれる流通制御情報を工夫することで実現できる。

【０１２０】

Ｆｔ≠１であれば（ステップＳ１４のＮＯ）、配信データメモリ２２０２への格納は禁止される（格納禁止）。

【０１２１】

ＩＤｔ≠ＩＤｔ”であれば（ステップＳ１３のＮＯ）、さらに、安全化データに含まれる所有者識別情報（ＩＤｕ）と携帯情報端末に記憶されている所有者識別情報（ＩＤｕ”）とを比較する（ステップＳ１５）。ＩＤｕ＝ＩＤｕ”であれば（ステップＳ１５のＹＥＳ）、安全化データに含まれる流通制御情報の同一所有者間移動フラグ（F_{ul}）の値が「１：許可」であるか否かを判定する（ステップＳ１６）。F_{ul}＝１であれば（ステップＳ１６のＹＥＳ）、上述したように配信データメモリ２２０２への格納が許可される（格納許可）。F_{ul}≠１であれば（ステップＳ１６のＮＯ）、配信データメモリ２２０２への格納は禁止される（格納禁止）。

【０１２２】

ＩＤｕ≠ＩＤｕ”であれば（ステップＳ１５のＮＯ）、さらに、安全化データに含まれる流通制御情報の異所有者間移動フラグ（F_{u2}）の値が「１：許可」であるか否かを判定する（ステップＳ１７）。F_{u2}＝１であれば（ステップＳ１７のＹＥＳ）、上述したように配信データメモリ２２０２への格納が許可される（格納許可）。F_{u2}≠１であれば（ステップＳ１７のＮＯ）、配信データメモリ２２０２への格納は禁止される（格納禁止）。

【０１２３】

以上説明した例では、安全化データ生成部２２０３と安全化データ更改部２１０９におけるコンテンツボディの暗号化、および、データ安全性確認部２２０６におけるコンテンツボディの復号において、公開鍵暗号系のコンテンツ暗号化鍵とコンテンツ復号鍵とを直接用いている。公開鍵暗号系に特有の計算速度の問題を解決するため、例えば、暗号化時に対称鍵暗号系の対称鍵をランダムに生成し、コンテンツボディは対称鍵を用いて暗号化し、当該対称鍵をコンテンツ暗号化鍵で暗号化して暗号化コンテンツボディと共に安全化データに含めてもよい。この場合、復号時には、まず、コンテンツ復号鍵で対称鍵を復号し、ここで得た対称鍵でコンテンツボディを復号することができる。

【０１２４】

システムの適用例

つぎに、本実施形態によるデジタル情報流通制御装置が想定する利用シーンの例を紹介する。

【０１２５】

図１３は本発明の第１実施形態によるデジタル情報流通制御システムの第１の適用例を示す概略的システム機能図である。図１３に示す利用シーンでは、システム管理者として携帯電話キャリア１０、サービス提供者として携帯電話向けサービス事業者１１、サービス利用者として携帯電話ユーザ１２を想定している。

【０１２６】

サービス提供者サーバ１は携帯電話２へ向けてコンテンツデータ（ここでは電子チケットを含むものとする。）を配信する。携帯電話ユーザ１２は配信されたコンテンツを携帯電話２上で閲覧したり、電子チケットサービスターミナル１３

が設置されている場所へ赴き、携帯電話２内の電子チケットを利用することができる。また、上述したように、携帯電話ユーザ１２は、赤外線通信や近距離無線通信などを利用して、自分のパーソナルコンピュータ３（ユーザ情報端末）にデジタルコンテンツや電子チケットをバックアップし、必要に応じて携帯電話２へリストアする。このバックアップおよびリストアは、上述したように正当性および安全性が担保されているために、ユーザの利便性とサービス提供者の権利保護とを共に確保することができる。

【０１２７】

システムの他の例

図１および図３に示す本発明の第１実施形態はハードウエアにより実現することもできるが、ソフトウエアによりコンピュータ上にインプリメントすることもできる。

【０１２８】

図１４は第１実施形態におけるサービス提供者サーバ１の他の例を示す概略的ブロック図であり、図１５は第１実施形態における携帯情報端末２およびユーザ情報端末３の他の例を示す概略的ブロック図である。なお、図１および図３に示すブロックと同じ機能を有するものには同一の参照番号を付して説明は省略する。

【０１２９】

図１４に示すように、サービス提供者サーバ１には、コンテンツ・流通制御情報メモリ１０１、サーバ固有情報メモリ１０３、プログラムメモリ１０５、プログラム制御プロセッサ１０８、通信制御部１０９および送受信部１１０が設けられている。プログラムメモリ１０５には、配信データ管理部１０２と同じ機能を実現する配信データ管理プログラム１０６と、安全化データ更新部１０４と同じ機能を実現する安全化データ更新プログラム１０７とが格納されている。

【０１３０】

プログラム制御プロセッサ１０８は、プログラムメモリ１０５に格納されたプログラムを実行することで、図２に示すような携帯情報端末２へのデータ配信、外部コンテンツ処理システム２４０１によるコンテンツデータの更新、更新リク

エストの受信、更新可否判定（ステップＳ０５）および安全化データの更新（ステップＳ０６）を実行する。特に、配信データ管理プログラム１０６を実行することによりデータ配信およびコンテンツデータの更新を実行する配信データ管理部１０２と、安全化データ更新プログラム１０７を実行することにより更新可否判定（ステップＳ０５）および安全化データの更新（ステップＳ０６）を実行する安全化データ更新部１０４と、をソフトウエア的に実現することができる。

【０１３１】

また、上述した更新リクエストの受信、更新安全化データの送信、配信データの送信などの実際の通信は、プログラム制御プロセッサ１０８の制御の下で通信制御部１０９および送受信部１１０により実行される。

【０１３２】

図１５に示すように、携帯情報端末２は、端末固有情報メモリ２０２、配信データメモリ２２０２、プログラムメモリ２０５、プログラム制御プロセッサ２０８、チャネル制御部２０９、送受信器２１０、通信制御部２１１、および、ワイヤード／ワイヤレスインタフェース２１２を有する。

【０１３３】

プログラムメモリ２０５には安全化データ検証プログラム２０６および安全化データ生成プログラム２０７が格納され、それぞれプログラム制御プロセッサ２０８により実行されることで、図２に示すような配信データの受信、配信データの保存／読み出し、安全化データ生成（ステップＳ０１）、安全化データリクエストの生成および送信、ユーザ情報端末３からの安全化データの受信、受信した安全化データの安全性確認、および、安全性が確認された配信データのリストアを実行する。特に、安全化データ生成プログラム２０７を実行することで安全化データ生成（ステップＳ０１）を実行するする安全化データ作成部２０３と、安全化データ検証プログラム２０６を実行することで安全性確認（ステップＳ０７）を実行する安全化データ検証部２０４とをソフトウエア的に実現することができる。サービス提供者サーバ１との通信はチャネル制御部２０９および送受信器２１０により実行し、ユーザ情報端末３との通信は通信制御部２１１およびインタフェース２１２により行う。

【０１３４】

また、ユーザ情報端末３は、安全化データメモリ３０１、ワイヤード／ワイヤレスインタフェース３０３、通信制御部３０４、プログラムメモリ３０５、プログラム制御プロセッサ３０７、通信制御部３０８、および、送受信部３０９を有する。プログラムメモリ３０５には安全化データ更新判定プログラム３０６が格納され、プログラム制御プロセッサ３０７により実行されることで、図１に示すようなバックアップ安全化データの受信、バックアップ安全化データの格納（ステップＳ０２）、安全化データリクエストの受信、更新判定（ステップＳ０３）、更新リクエストの生成（ステップＳ０４）、および、更新安全化データの受信および転送を実行する。とくに、安全化データ更新判定プログラム３０６を実行することにより、更新判定（ステップＳ０３）を実行する安全化データ更新判定部３０２をソフトウエア的に実現することができる。サービス提供者サーバ１との通信は通信制御部３０８および送受信部３０９により実行し、携帯情報端末２との通信は通信制御部３０４およびインタフェース３０３により行う。

【０１３５】

２．第２実施形態

携帯情報端末２に格納された配信データを安全化データとしてバックアップし、必要に応じてリストアするシステムは、図１に示すような携帯情報端末２とユーザ情報端末３とを直接接続した構成に限定されるものではない。本発明によるバックアップおよびリストア動作は、携帯情報端末２とユーザ情報端末３とがネットワークを介して接続されたシステム構成においても可能である。

【０１３６】

図１６は本発明の第２実施形態によるデジタル情報流通制御システムの概略的機能構成を示すブロック図である。本実施形態によるシステムでは、図１におけるユーザ情報端末がネットワーク５に接続されたバックアップサーバ３により実現されている。バックアップサーバ３の基本構成および動作は、第１実施形態のユーザ情報端末３と同じであるから説明は省略する。

【０１３７】

図１７は本発明の第２実施形態によるデジタル情報流通制御システムの適用例

を示す概略的システム機能図である。図１７に示す利用シーンでは、ユーザ情報端末が携帯電話ユーザ１２のパーソナルコンピュータではなく、バックアップサービス事業者１４が管理するバックアップサーバ３である。本発明によるバックアップやリストアは公衆網を介して行われる。

【０１３８】

３．第３実施形態

図１および図３に示す第１実施形態では、ユーザ情報端末３が、サービス提供者サーバ１へインターネットなどのネットワーク５で接続され、安全化データの更新ができる場合を説明した。しかしながら、本発明はこのような構成に限定されるものではない。たとえば、安全化データ更新判定部３０２に含まれる更新要否判定機能、更新リクエスト生成機能、更新リクエスト送信機能などを携帯情報端末２に持たせることもできる。この場合には、ユーザ情報端末３はサービス提供者サーバ１へ接続する通信機能が不要となる。

【０１３９】

図１８は本発明の第３実施形態によるデジタル情報流通制御システムを示す概略的システム機能図である。なお、図１および図３に示すブロックと同じ機能を有するものには同一の参照番号を付して説明は省略する。図１９は、図１８のデジタル情報流通制御システムの全体的なシーケンシャル動作および各端末およびサーバの概略的動作フローを示す流れ図である。なお図２に示す流れ図と同じ動作ステップには同じ参照番号を付している。

【０１４０】

図１８および図１９に示すように、本実施形態における携帯情報端末２には、安全化データ更新判定部２２０が設けられ、ユーザ情報端末３には安全化データ格納部３０１の一般的なデータ入出力制御を行う制御部３１０が設けられている。配信データが携帯情報端末２の配信データ格納部２０１に格納され、バックアップ時には配信データと端末固有情報とを利用してバックアップ用の安全化データが作成され（ステップＳ０１）、ユーザ情報端末３の安全化データ格納部３０１に格納される（ステップＳ０２）。

【０１４１】

リストア時に携帯情報端末２から安全化データリクエストがユーザ情報端末３へ出力され、それにより制御部３１０は安全化データ格納部３０１から対応するバックアップ安全化データを読み出し、携帯情報端末２の安全化データ更新判定部２２０へ送信する。安全化データ更新判定部２２０は、安全化データリクエストの識別情報とバックアップ安全化データの識別情報および流通制御情報とを用いて、バックアップ安全化データをそのまま使用できるか否か、それともサービス提供者サーバ１への問い合わせが必要か否かを判断する（ステップＳ００１）。すなわち、ステップＳ００１は図２のステップＳ０３を同様の動作を行う。バックアップ安全化データをそのまま使用できる場合は、上述した検証（ステップＳ０７）を経て配信データ格納部２０１にリストアされる。

【０１４２】

問い合わせが必要であれば、バックアップ安全化データおよび安全化データリクエストから更新リクエストを生成し（ステップＳ００２）、送受信部２２１を通してサービス提供者サーバ１へ送信する。サービス提供者サーバ１から更新安全化データが帰ってくると、それを安全化データ検証部２０４へ出力し、上述した検証（ステップＳ０７）を経て配信データ格納部２０１にリストアされる。

【０１４３】

４．第４実施形態

図１１（Ａ）および（Ｂ）において説明したように、サービス提供者によって更新された安全化データにはサービス提供者更新フラグ（Ｆ）が設定されている。第１実施形態ではこの更新フラグＦによって更新の有無を判定したが、単に更新の有無を示すフラグとしてだけでなく、安全化データのリストア可能な有効期限を示す情報としても利用することができる。

【０１４４】

本発明の第４実施形態では、サービス提供者サーバ１において更新安全化データに有効期限情報が付加される。この場合のデータ安全性確認部２２０６の動作は次のようになる。

【０１４５】

図２０は、有効期限情報を含む更新安全化データを受信したときのデータ安全

性確認部２２０６のデータ安全性確認動作の一例を示すフローチャートである。なお、図１２のフローチャートと同じステップは同じ参照番号を付して説明は省略する。

【０１４６】

ユーザ情報端末３から受信した安全化データに更新フラグＦが含まれている場合には（ステップＳ１１のＹＥＳ）、データ安全性確認部２２０６はその更新フラグＦに付加された有効期限情報を読み取り、携帯情報端末２内の時計から読み出した現時刻情報と比較する（ステップＳ２０）。現時刻が更新安全化データの有効期限内であれば（ステップＳ２０のＹＥＳ）、ステップＳ１２が実行され、上述したように更新安全化データの格納が禁止あるいは許可される。現時刻が更新安全化データの有効期限を超えていれば（ステップＳ２０のＮＯ）、更新安全化データの格納は禁止される。

【０１４７】

このように、サービス提供者更新フラグＦの有効期限情報を参照してリストアの可否を判定することにより、安全化データ更改部２１０９で生成した安全化データを悪意ある利用者がユーザ情報端末３に蓄積し、有効期限を超えて携帯情報端末２へ繰り返しリストアすることを防止できる。上述したように、サービス提供者サーバ１で更新された安全化データを悪意のプログラムが盗み、それを同一の携帯情報端末にリストアすることは可能である。このような不正なリストアを防止するために、サービス提供者更新フラグＦに設定される有効期限をたとえば安全化データの更新から１０秒後などの非常に短時間に設定することは有効である。

【０１４８】

５．第５実施形態

第１実施形態で説明したように、ユーザ情報端末３に保存されているバックアップ安全化データをリストアしようとする際、携帯情報端末２の安全化データリクエスト生成部２２０４は、端末識別情報（ＩＤｔ’）、所有者識別情報（ＩＤｕ’）、および、必要に応じてコンテンツ暗号化鍵（ｅｋ’）およびコンテンツ暗号化鍵証明書（ｃ＿ｅｋ’）を含む安全化データリクエストを生成する（図８

参照）。さらに、この安全化データリクエスト自体に固有情報を付加することで、不正なリストアを有効に防止することが可能である。

【０１４９】

図２１は本発明の第５実施形態における安全化データリクエストの構成例を示す模式図である。本実施形態における安全化データリクエストは、端末識別情報（ＩＤｔ’）、所有者識別情報（ＩＤｕ’）、コンテンツ暗号化鍵（ｅｋ’）、コンテンツ暗号化鍵証明書（ｃ＿ｅｋ’）、および、乱数ｒを含んで構成される。

【０１５０】

本実施形態における安全化データリクエスト生成部２２０４は、乱数発生器から発生した乱数ｒを入力して安全化データリクエストに付加すると共に、この乱数ｒを保持しておく。乱数ｒを含む安全化データリクエストがユーザ情報端末３へ送信され、サーバ問合せが必要であれば、更新リクエスト生成部２３０４はバックアップ安全化データと安全化データリクエストとを組み合わせた更新リクエストを生成する（図１０参照）。したがって、本実施形態では、更新リクエストの安全化データリクエストの部分には乱数ｒが含まれている。この更新リクエストがサービス提供者サーバ１へ送信される。

【０１５１】

図１１（Ａ）および（Ｂ）において説明したように、サービス提供者によって更新された安全化データにはサービス提供者更新フラグ（Ｆ）が設定されている。第１実施形態ではこの更新フラグＦによって更新の有無を判定したが、単に更新の有無を示すフラグとしてだけでなく、乱数ｒを示す情報としても利用することができる。本実施形態では、サービス提供者サーバ１において更新安全化データの更新フラグＦに乱数ｒの情報が付加される。この場合のデータ安全性確認部２２０６の動作は次のようになる。

【０１５２】

図２２は、乱数ｒを含む更新安全化データを受信したときのデータ安全性確認部２２０６のデータ安全性確認動作の一例を示すフローチャートである。なお、図１２のフローチャートと同じステップは同じ参照番号を付して説明は省略する

。

【０１５３】

ユーザ情報端末３から受信した安全化データに更新フラグＦが含まれている場合には（ステップＳ１１のＹＥＳ）、データ安全性確認部２２０６はその更新フラグＦに付加された乱数ｒ’を読み取り、安全化データリクエスト生成時に保持された乱数ｒ”と比較する（ステップＳ２１）。ｒ’＝ｒ”であれば（ステップＳ２１のＹＥＳ）、ステップＳ１２が実行され、上述したように更新安全化データの格納が禁止あるいは許可される。ｒ’≠ｒ”であれば（ステップＳ２１のＮＯ）、更新安全化データの格納は禁止される。

【０１５４】

このように、サービス提供者更新フラグＦの乱数情報を参照してリストアの可否を判定することにより、安全化データ更改部２１０９で生成した安全化データを悪意ある利用者がユーザ情報端末３に蓄積し、携帯情報端末２へ繰り返しリストアすることを防止できる。本実施形態では、携帯情報端末２に信頼できる時計がない場合でも不正なリストアを有効に防止できる。

【０１５５】

６．第６実施形態

流通制御情報の他の例

図６（Ａ）に示す流通制御情報（Ｐ）は、図６（Ｂ）に示すようなフラグ構成だけではない。流通制御情報（Ｐ）をプログラムの関数として手続き的に記述することも可能である。

【０１５６】

図２３は、プログラムの関数として記述した流通制御情報の一例を示す模式図である。ここでは、流通制御情報がＣ＋＋プログラミング言語で記述されており、「端末識別情報が一致した場合にはリストア許可、サービス提供者が指定する特別な日（ここでは２００４年２月１４日）に所有者識別情報が一致した場合にはサーバ問い合わせ後リストア許可、それ以外はリストア不許可」という内容の流通制御を行うことができる。

【０１５７】

このようにプログラムで流通制御情報を記述した場合には、更新要否判定部２３０３およびデータ安全性確認部２２０６は、この流通制御プログラムを読み込んで実行することとなり、図９および図１２に示すフラグベースの更新要否判定およびデータ安全性確認に比べて柔軟な流通制御が可能となる。

【０１５８】

【発明の効果】

以上詳細に説明したように、本発明によれば、サービス提供者がコンテンツデータに流通制御情報を付加して配信することにより、コンテンツデータの流通を制御することができる。たとえば、流通制御情報の設定により、サーバへの更新判定問い合わせ、あるいは、更新なしの安全化データリストアを選択することができ、ネットワークおよびサーバの負荷の増大を抑制できる。さらに、流通制御情報を用いることで、配信データのバックアップおよびリストアの正当性を確実に判定することができ、利用者の利益とサービス提供者の利益とを両立させることができる。特に、デジタル署名および暗号化技術を用いてデータ転送および検証を行うことで、より確かな正当性判定およびデータ保護が可能となる。また、流通制御情報の設定によりデータ転送が制御可能であるから、バックアップおよびリストアするための条件を柔軟に設定できる。

【０１５９】

また、携帯情報端末へリストアされるコンテンツデータ（たとえば電子チケット）がサービス提供者サーバで管理するコンテンツデータと一致することを保証する流通制御情報を設定し、携帯情報端末に格納されているコンテンツデータが正しいことを保証できる。このため、コンテンツデータをチェックしてデジタル情報や物品の提供／貸与管理、乗車／乗船などの入場管理を実施する際に、サービス提供者サーバに問い合わせることなく、コンテンツデータを信頼して提供／貸与、入場管理を行うことができる。紛失などに伴うリストア操作は、通常のコンテンツデータ利用操作に比べ、圧倒的にその回数が少ないと考えられるため、サービス提供者が運営する電子チケットサーバの負荷を大幅に軽減することができる。

【０１６０】

さらに、システム管理者は、サービス提供者へサービス提供者ＩＤやサービス提供者証明書を発行し、携帯情報端末へ端末識別情報やユーザＩＤ、端末証明書などを発行、格納する処理を、サービス提供者がサービスを立ち上げるとき、及び、サービス利用者が新たな携帯情報端末の利用を開始するときに実施すればよい。したがって、サービス利用者がデジタルコンテンツや電子チケットのバックアップやリストアを実行する度に実施すべき処理はない。このため、多数のサービス提供者、多数の携帯情報端末が存在し、膨大なデジタルコンテンツや電子チケットが流通する環境においても、システム管理者が実施する処理はサービス提供者数と携帯情報端末数に比例しており、スケーラビリティに優れたデジタル情報流通制御を実現することができる。

【０１６１】

また、ユーザ情報端末へバックアップしたデジタルコンテンツや電子チケットは、必要に応じて暗号化されており、ユーザ情報端末における閲覧や不正コピーを防止できる。また、ユーザ情報端末において改ざんしたデータは携帯情報端末へリストアできないため、サービス提供者は安心して、サービス利用者にデジタルコンテンツや電子チケットのバックアップとリストアを許可することが可能になる。このためサービス利用者は、携帯情報端末の紛失に備えたバックアップやリストアが可能となり、利便性が向上する。

【図面の簡単な説明】

【図１】

本発明の第１実施形態によるデジタル情報流通制御システムの概略的機能構成を示すブロック図である。

【図２】

図１のデジタル情報流通制御システムの全体的なシーケンシャル動作および各端末およびサーバの概略的動作フローを示す流れ図である。

【図３】

図１に示すデジタル情報流通制御システムのより詳細な機能構成を示すブロック図である。

【図４】

携帯情報端末２の端末固有情報格納部２０２に格納される端末固有情報を示す模式図である。

【図５】

サービス提供者サーバ１のサーバ固有情報格納部１０３に格納されるサーバ固有情報を示す模式図である。

【図６】

（Ａ）は配信データ生成部２１０３で生成される配信データの構成の一例を示す模式図であり、（Ｂ）はその流通制御情報の記述例を示す模式図である。

【図７】

（Ａ）は、安全化データ生成部２２０３で生成され、送信時にコンテンツボディの暗号化を行わないと指定されたバックアップ用安全化データの構成例を示す模式図であり、（Ｂ）は、安全化データ生成部２２０３で生成され、送信時にコンテンツボディの暗号化を行うと指定されたバックアップ用安全化データの構成例を示す模式図である。

【図８】

安全化データリクエスト生成部２２０４で生成する安全化データリクエストの構成例を示す模式図である。

【図９】

更新要否判定部２３０３の安全化データ更新判定動作の一例を示すフローチャートである。

【図１０】

更新リクエストの構成例を示す模式図である。

【図１１】

（Ａ）は、安全化データ更改部２１０９で生成され、送信時にコンテンツボディの暗号化を行わないと指定された更新安全化データの構成例を示す模式図であり、（Ｂ）は、安全化データ更改部２１０９で生成され、送信時にコンテンツボディの暗号化を行うと指定された更新安全化データの構成例を示す模式図である。

【図１２】

データ安全性確認部２２０６におけるデータ安全性確認動作の一例を示すフローチャートである。

【図１３】

本発明の第１実施形態によるデジタル情報流通制御システムの第１の適用例を示す概略的システム機能図である。

【図１４】

第１実施形態におけるサービス提供者サーバ１の他の例を示す概略的ブロック図である。

【図１５】

第１実施形態における携帯情報端末２およびユーザ情報端末３の他の例を示す概略的ブロック図である。

【図１６】

本発明の第２実施形態によるデジタル情報流通制御システムの概略的機能構成を示すブロック図である。

【図１７】

本発明の第２実施形態によるデジタル情報流通制御システムの適用例を示す概略的システム機能図である。

【図１８】

本発明の第３実施形態によるデジタル情報流通制御システムを示す概略的システム機能図である。

【図１９】

図１８のデジタル情報流通制御システムの全体的なシーケンシャル動作および各端末およびサーバの概略的動作フローを示す流れ図である。

【図２０】

有効期限情報を含む更新安全化データを受信したときのデータ安全性確認部２２０６のデータ安全性確認動作の一例を示すフローチャートである。

【図２１】

本発明の第５実施形態における安全化データリクエストの構成例を示す模式図である。

【図２２】

乱数ｒを含む更新安全化データを受信したときのデータ安全性確認部２２０６のデータ安全性確認動作の一例を示すフローチャートである。

【図２３】

本発明の第６実施形態における流通制御情報の一例を示す模式図である。

【符号の説明】

１　サービス提供者サーバ

２　携帯情報端末

３　ユーザ情報端末

４，５　ネットワーク

１０１　コンテンツ・流通制御情報格納部

１０２　配信データ管理部

１０３　サーバ固有情報格納部

１０４　安全化データ更新部

２０１　配信データ格納部

２０２　端末固有情報格納部

２０３　安全化データ作成部

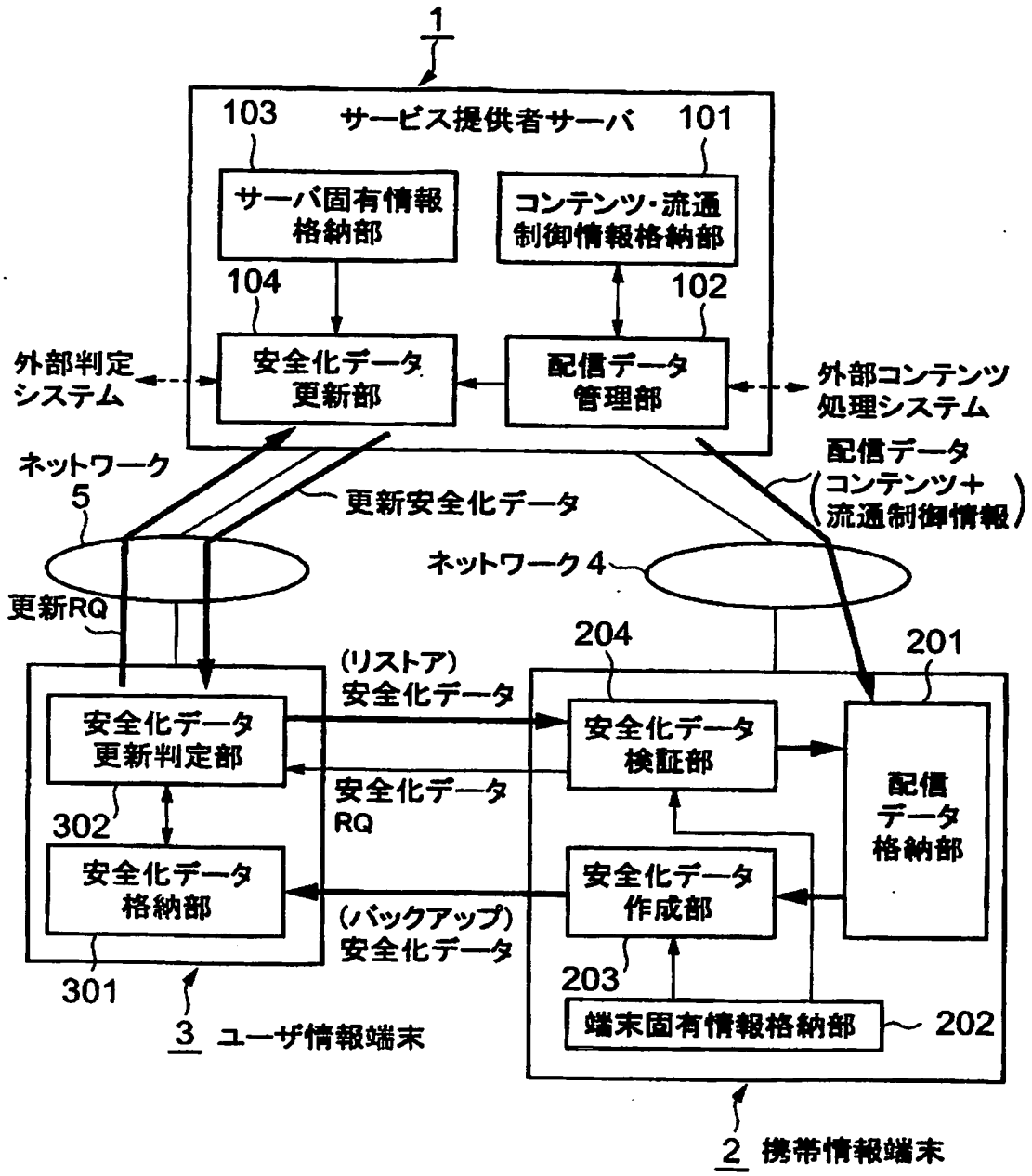
２０４　安全化データ検証部

３０１　安全化データ格納部

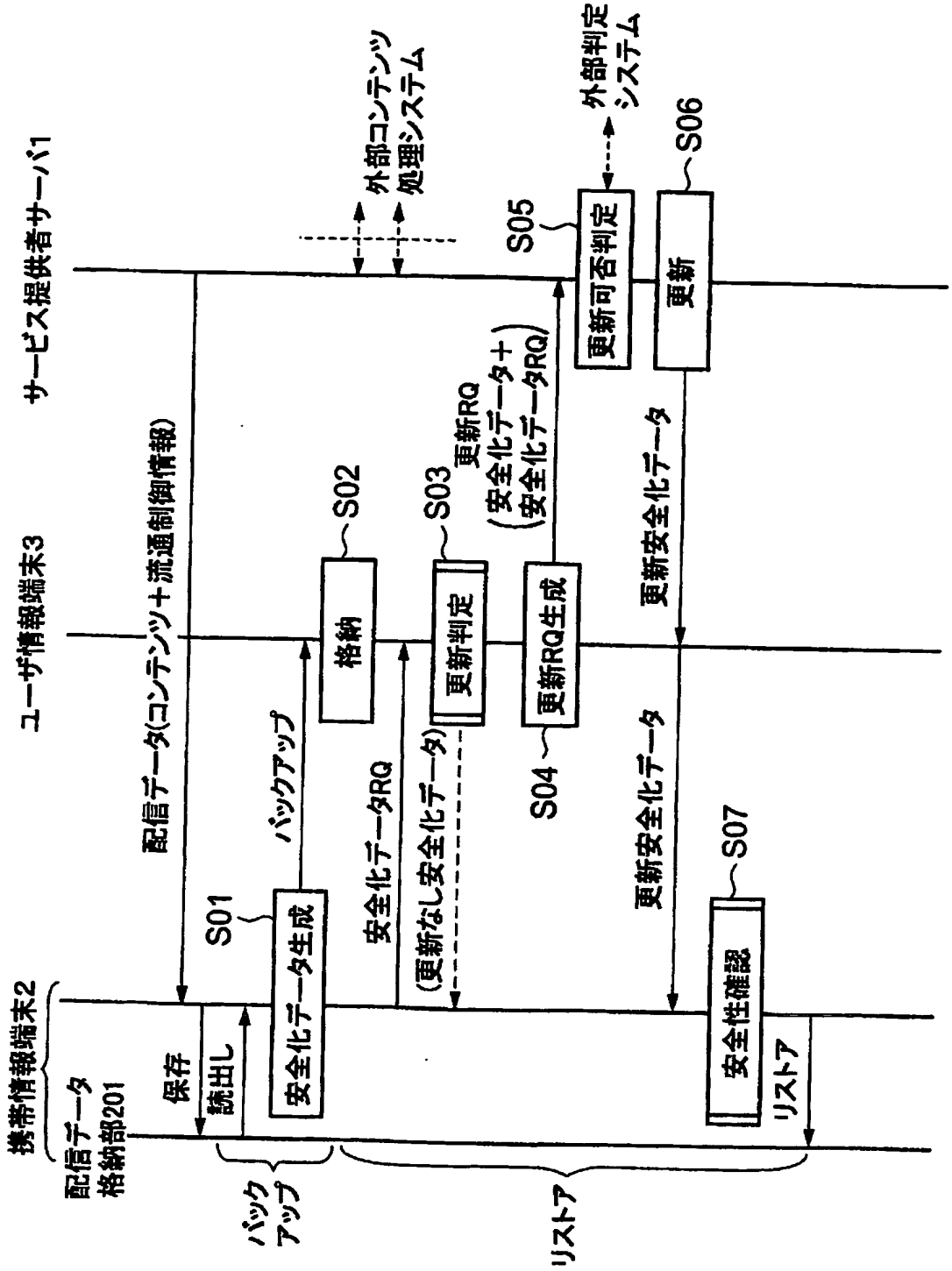
３０２　安全化データ更新判定部

【書類名】　図面

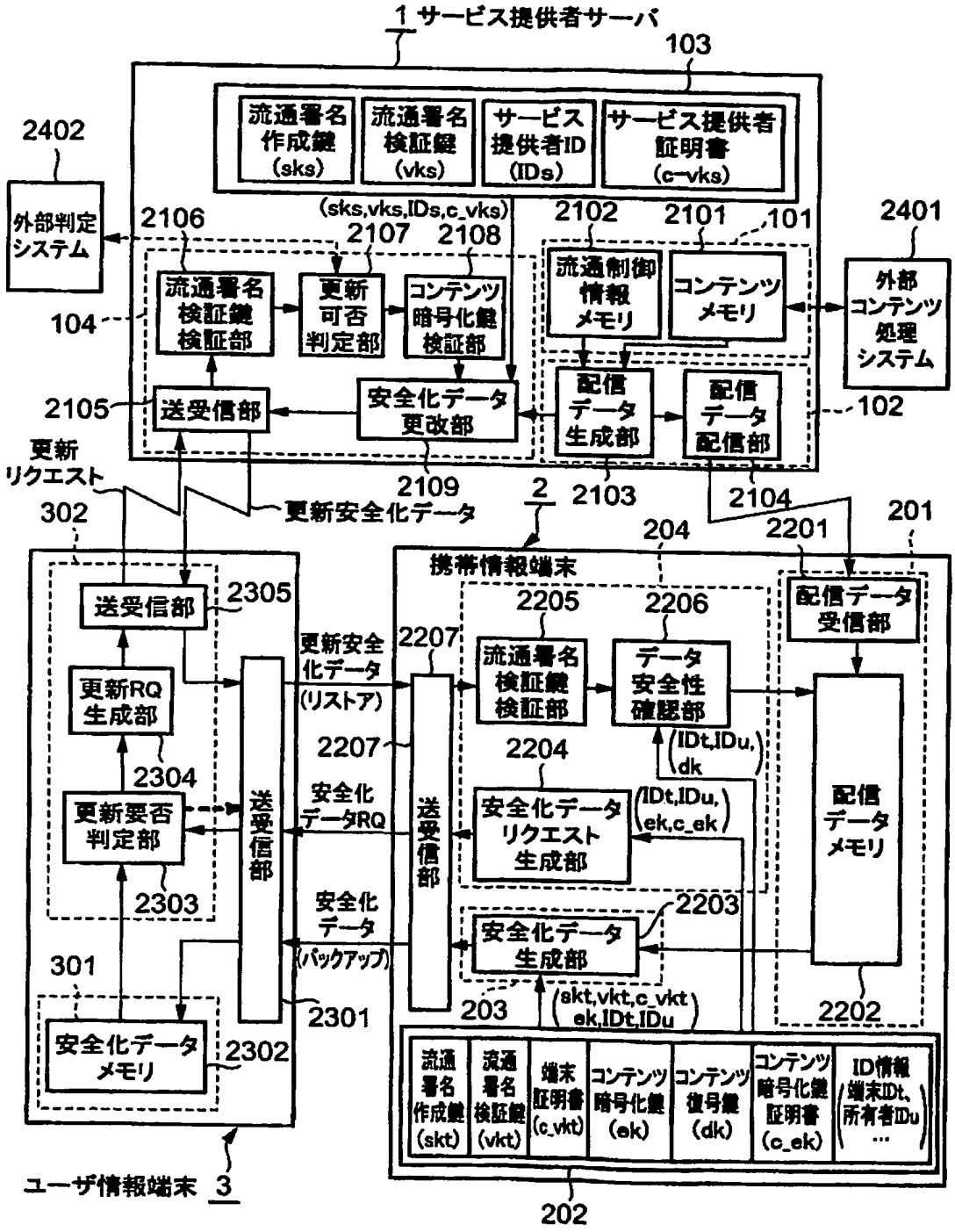
【図１】


1
103
サービス提供者サーバ
101
サーバ固有情報格納部
コンテンツ・流通制御情報格納部
104
102
外部判定システム
安全化データ更新部
配信データ管理部
外部コンテンツ処理システム
ネットワーク5
更新安全化データ
配信データ（コンテンツ＋流通制御情報）
ネットワーク4
更新RQ
204
201
（リストア）安全化データ
安全化データ更新判定部
安全化データ検証部
安全化データRQ
302
配信データ格納部
安全化データ格納部
安全化データ作成部
（バックアップ）安全化データ
301
203
端末固有情報格納部
202
3 ユーザ情報端末
2 携帯情報端末

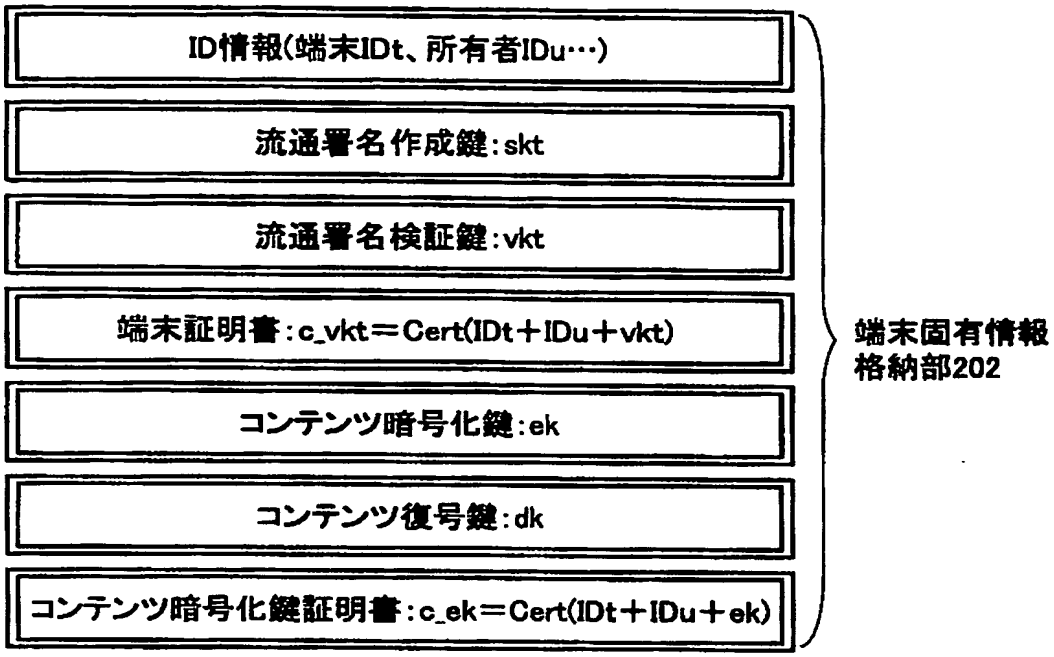
【図２】


サービス提供者サーバ1
ユーザ情報端末3
携帯情報端末2
配信データ
格納部201
外部コンテンツ
処理システム
外部判定
システム
配信データ(コンテンツ＋流通制御情報)
S01
保存
読出し
安全化データ生成
バックアップ
S02
格納
安全化データRQ
S03
更新判定
(更新なし安全化データ)
更新RQ
(安全化データ＋
安全化データRQ)
S04
更新RQ生成
S05
更新可否判定
S06
更新
更新安全化データ
更新安全化データ
S07
安全性確認
リストア
バック
アップ
リストア

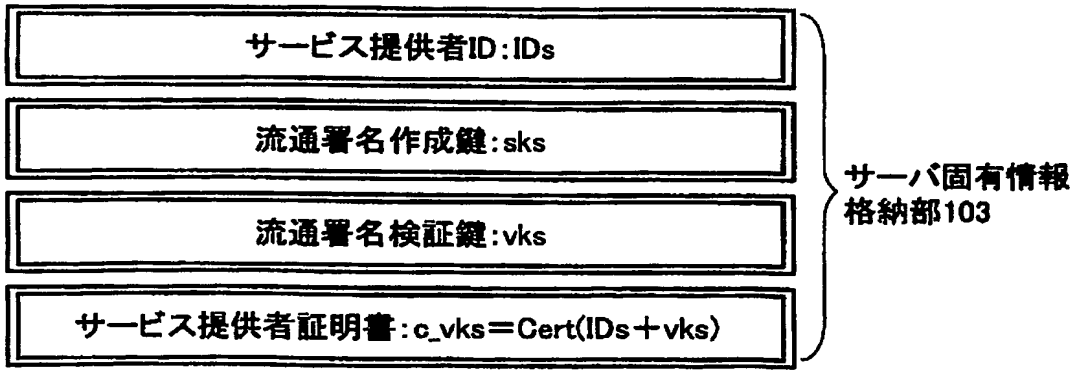
【図３】


1 サービス提供者サーバ
103
流通署名作成鍵 (sks)
流通署名検証鍵 (vks)
サービス提供者ID (IDs)
サービス提供者証明書 (c-vks)
2402
外部判定システム
2106
(sks,vks,IDs,c_vks)
2107
2108
2102
2101
101
2401
流通署名検証鍵検証部
更新可否判定部
コンテンツ暗号化鍵検証部
流通制御情報メモリ
コンテンツメモリ
外部コンテンツ処理システム
104
2105
送受信部
安全化データ更改部
配信データ生成部
配信データ配信部
102
更新リクエスト
更新安全化データ
2109
2
2103
2104
302
204
2201
201
携帯情報端末
送受信部
2305
2205
2206
配信データ受信部
更新安全化データ (リストア)
2207
流通署名検証鍵検証部
データ安全性確認部
更新RQ生成部
2207
2204
(IDt,IDu, dk)
2304
安全化データRQ
安全化データリクエスト生成部
(IDt,IDu, ek,c_ek)
配信データメモリ
更新要否判定部
送受信部
送受信部
2303
安全化データ (バックアップ)
2203
安全化データ生成部
301
2301
203
(skt,vkt,c_vkt ek,IDt,IDu)
2202
安全化データメモリ
2302
流通署名作成鍵 (skt)
流通署名検証鍵 (vkt)
端末証明書 (c_vkt)
コンテンツ暗号化鍵 (ek)
コンテンツ復号鍵 (dk)
コンテンツ暗号化鍵証明書 (c_ek)
ID情報 (端末IDt, 所有者IDu …)
ユーザ情報端末 3
202

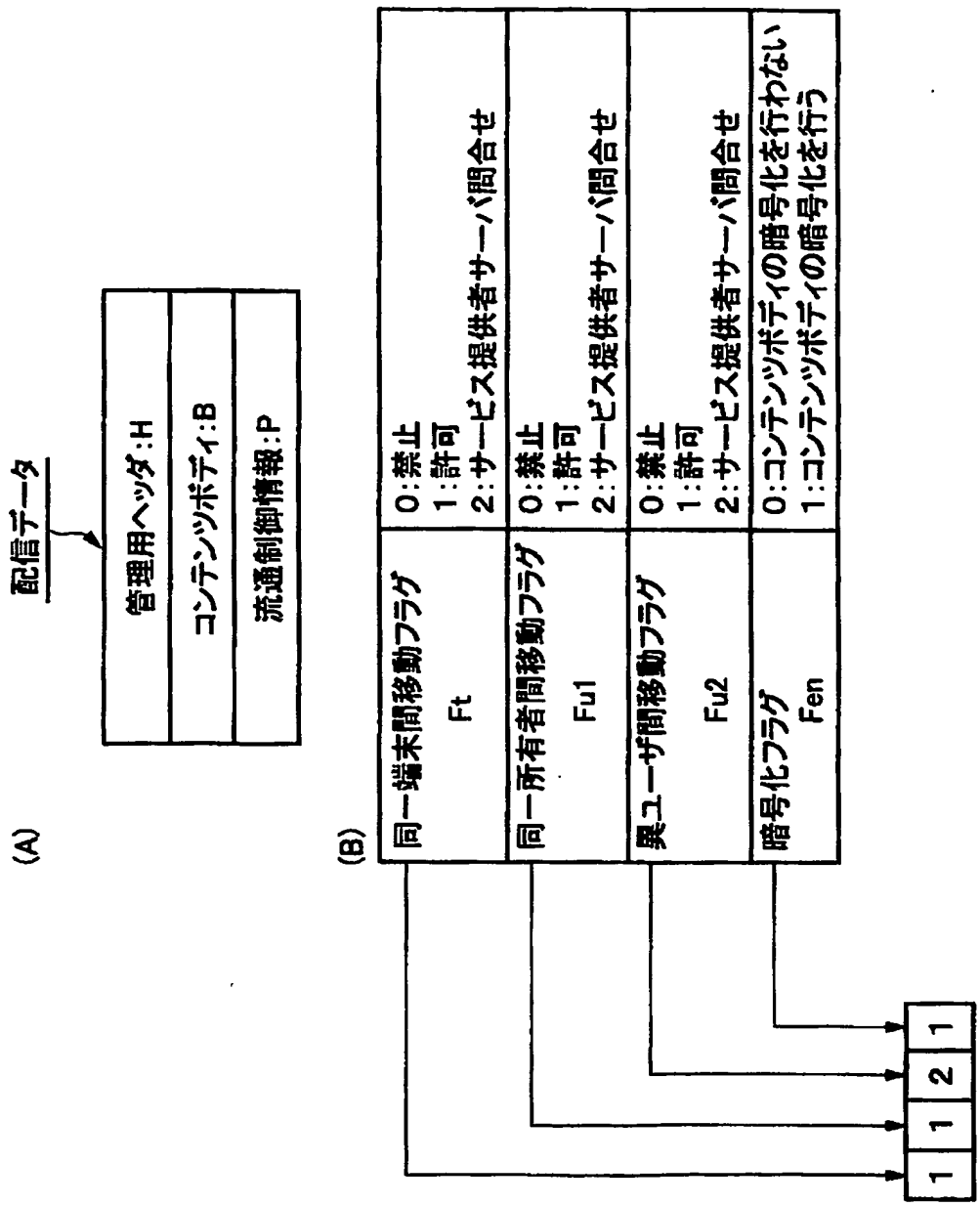
【図４】


ID情報(端末IDt、所有者IDu…)
流通署名作成鍵:skt
流通署名検証鍵:vkt
端末証明書:c_vkt＝Cert(IDt＋IDu＋vkt)
コンテンツ暗号化鍵:ek
コンテンツ復号鍵:dk
コンテンツ暗号化鍵証明書:c_ek＝Cert(IDt＋IDu＋ek)
端末固有情報
格納部202

【図５】

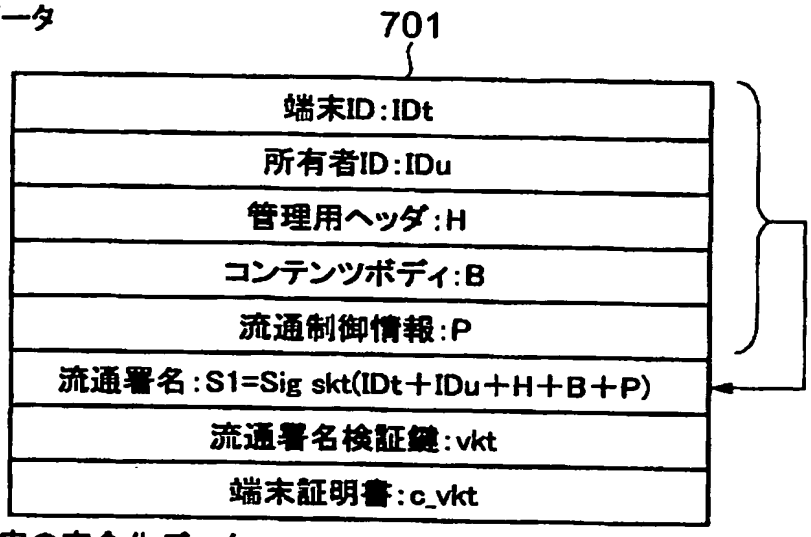

サービス提供者ID:IDs
流通署名作成鍵:sks
流通署名検証鍵:vks
サービス提供者証明書:c_vks＝Cert(IDs＋vks)
サーバ固有情報
格納部103

【図６】

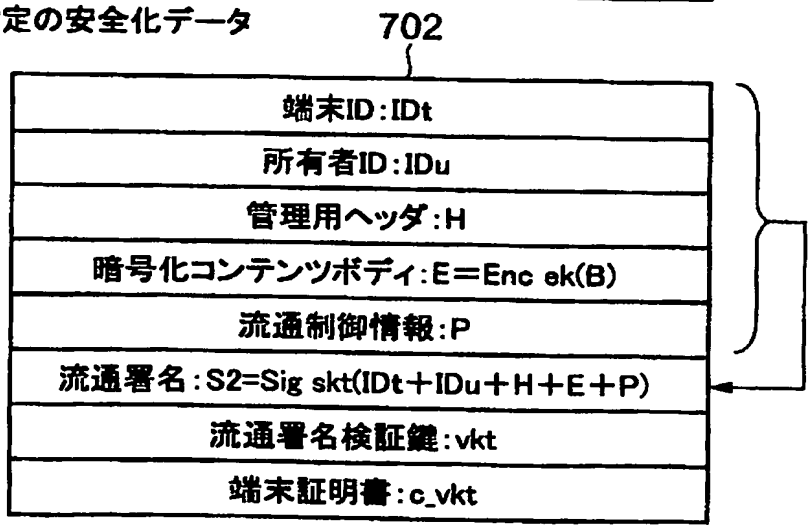

(A)
配信データ
管理用ヘッダ:H
コンテンツボディ:B
流通制御情報:P
(B)
同一端末間移動フラグ
Ft
0:禁止
1:許可
2:サービス提供者サーバ問合せ
同一所有者間移動フラグ
Fu1
0:禁止
1:許可
2:サービス提供者サーバ問合せ
異ユーザ間移動フラグ
Fu2
0:禁止
1:許可
2:サービス提供者サーバ問合せ
暗号化フラグ
Fen
0:コンテンツボディの暗号化を行わない
1:コンテンツボディの暗号化を行う
1
1
2
1

【図７】

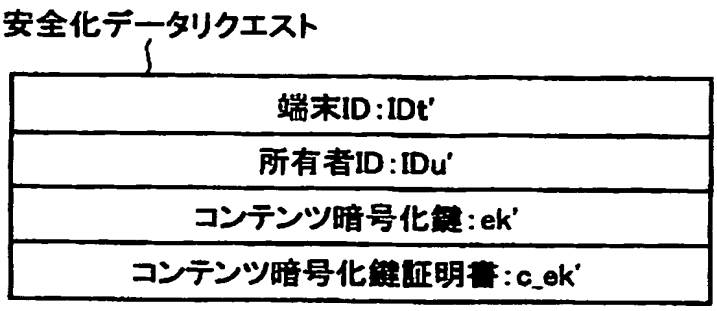
(A) 安全化データ



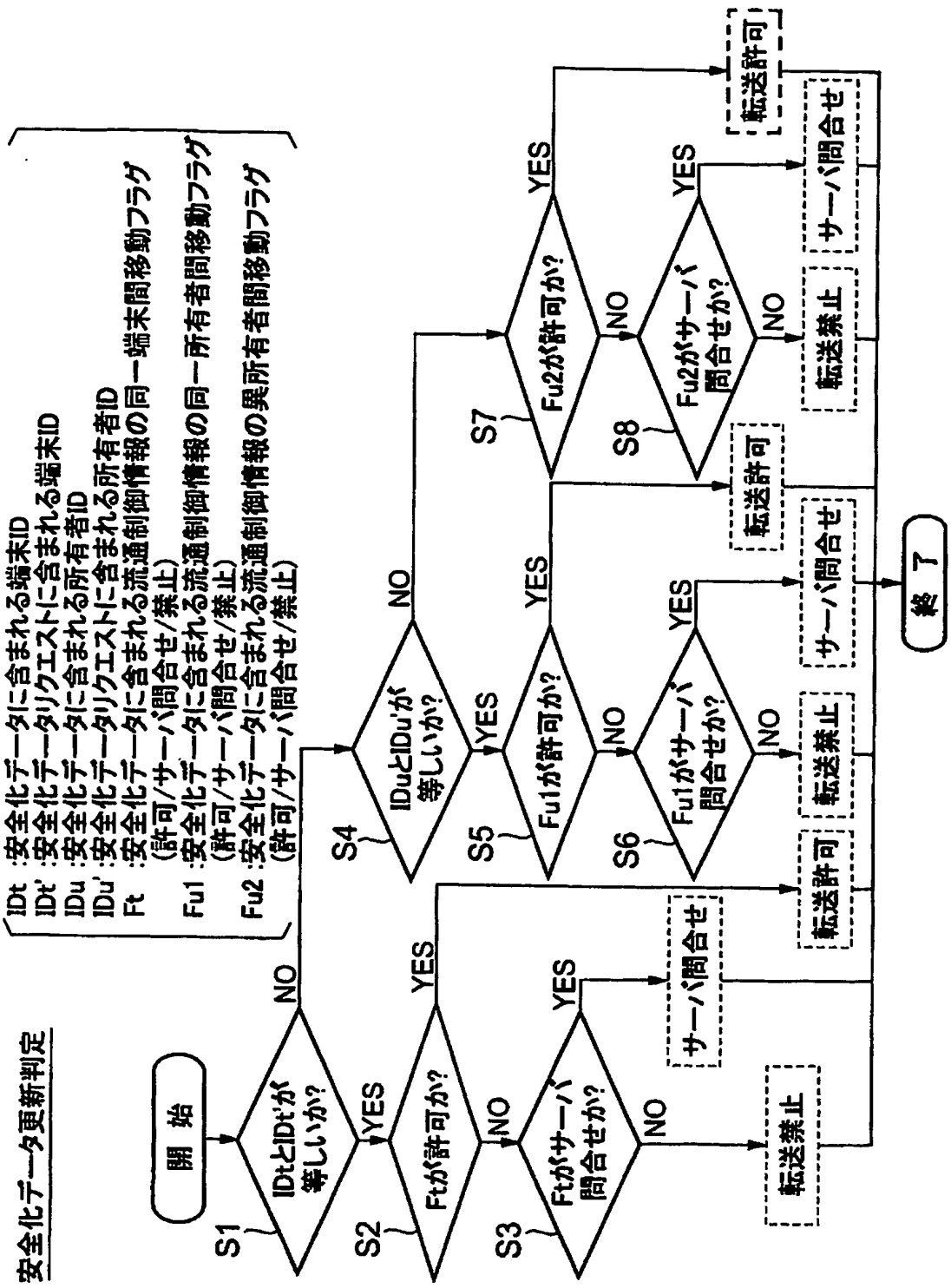
(B) 暗号化指定の安全化データ



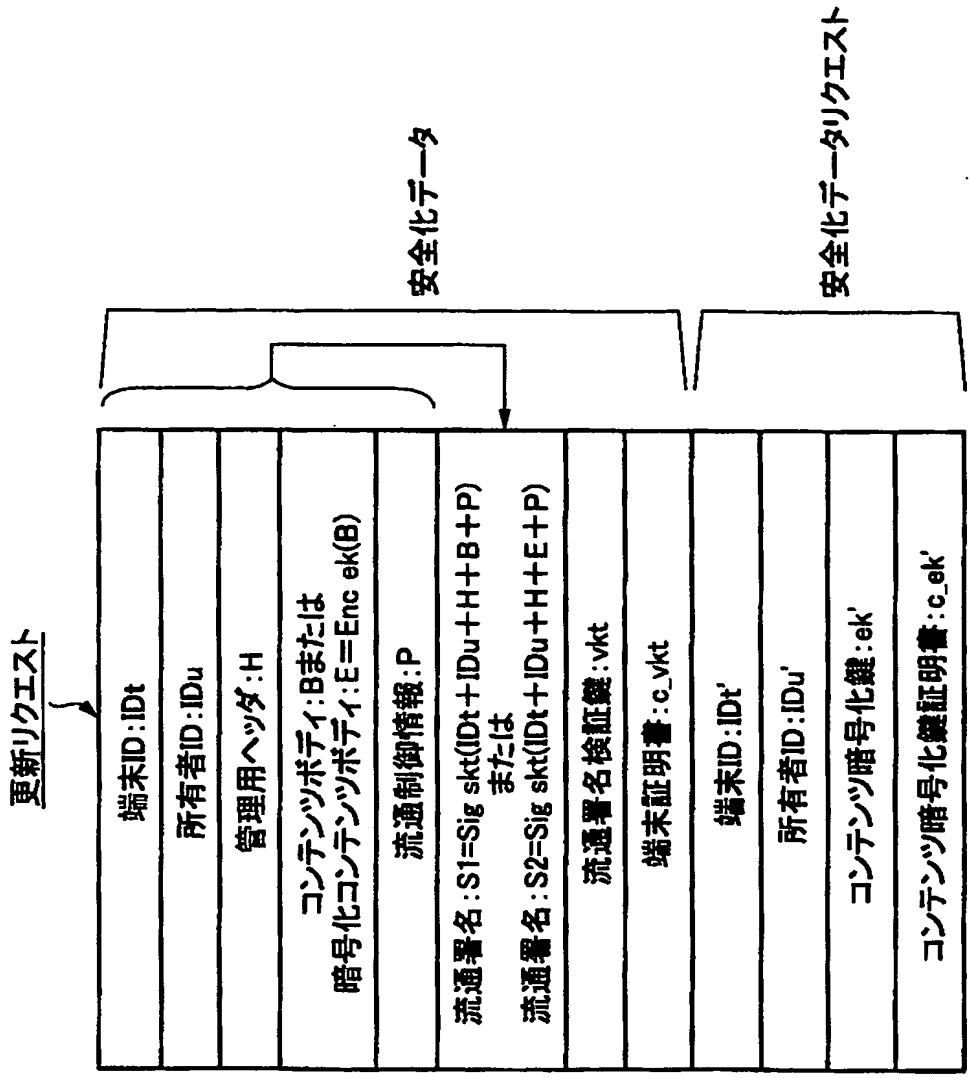
【図８】


安全化データリクエスト
端末ID:IDt'
所有者ID:IDu'
コンテンツ暗号化鍵:ek'
コンテンツ暗号化鍵証明書:c_ek'

【図９】

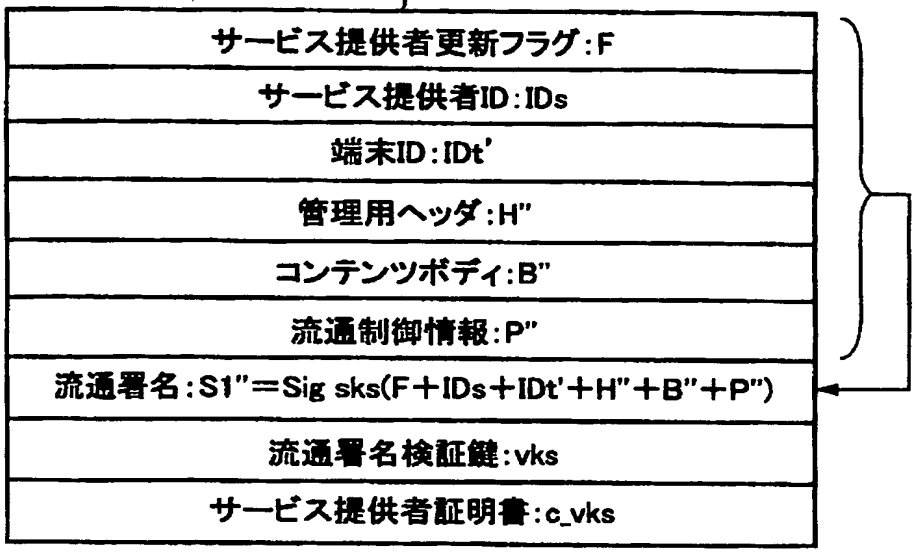

安全化データ更新判定
IDt :安全化データに含まれる端末ID
IDt' :安全化データリクエストに含まれる端末ID
IDu :安全化データに含まれる所有者ID
IDu' :安全化データリクエストに含まれる所有者ID
Ft :安全化データに含まれる流通制御情報の同一端末間移動フラグ (許可/サーバ問合せ/禁止)
Fu1 :安全化データに含まれる流通制御情報の同一所有者間移動フラグ (許可/サーバ問合せ/禁止)
Fu2 :安全化データに含まれる流通制御情報の異所有者間移動フラグ (許可/サーバ問合せ/禁止)
開 始
S1
IDtとIDt'が等しいか?
NO
YES
S2
Ftが許可か?
NO
YES
S3
Ftがサーバ問合せか?
NO
YES
S4
IDuとIDu'が等しいか?
NO
YES
S5
Fu1が許可か?
NO
YES
S6
Fu1がサーバ問合せか?
NO
YES
S7
Fu2が許可か?
NO
YES
S8
Fu2がサーバ問合せか?
NO
YES
転送禁止
サーバ問合せ
転送許可
終 了

【図１０】

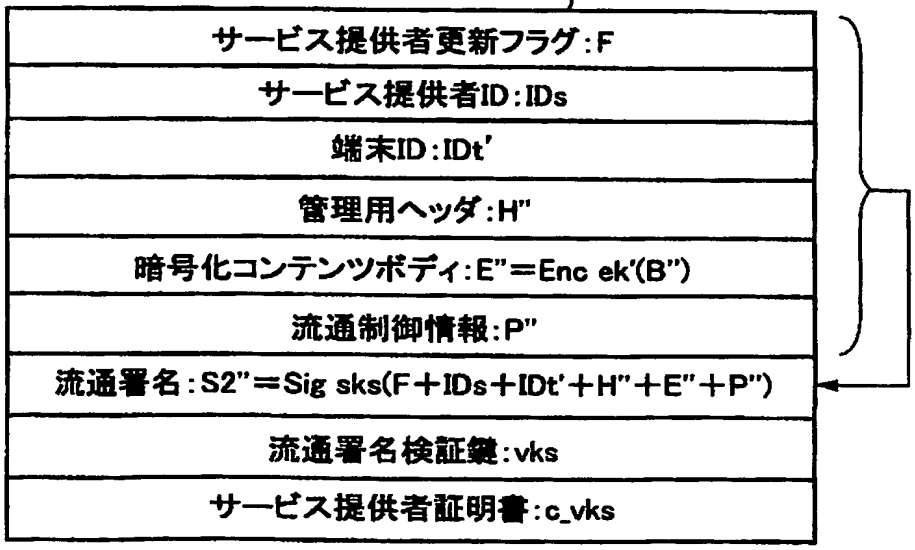

更新リクエスト
端末ID:IDt
所有者ID:IDu
管理用ヘッダ:H
コンテンツボディ:Bまたは
暗号化コンテンツボディ:E=Enc ek(B)
流通制御情報:P
流通署名:S1=Sig skt(IDt+IDu+H+B+P)
または
流通署名:S2=Sig skt(IDt+IDu+H+E+P)
流通署名検証鍵:vkt
端末証明書:c_vkt
端末ID:IDt'
所有者ID:IDu'
コンテンツ暗号化鍵:ek'
コンテンツ暗号化鍵証明書:c_ek'
安全化データ
安全化データリクエスト

【図１１】

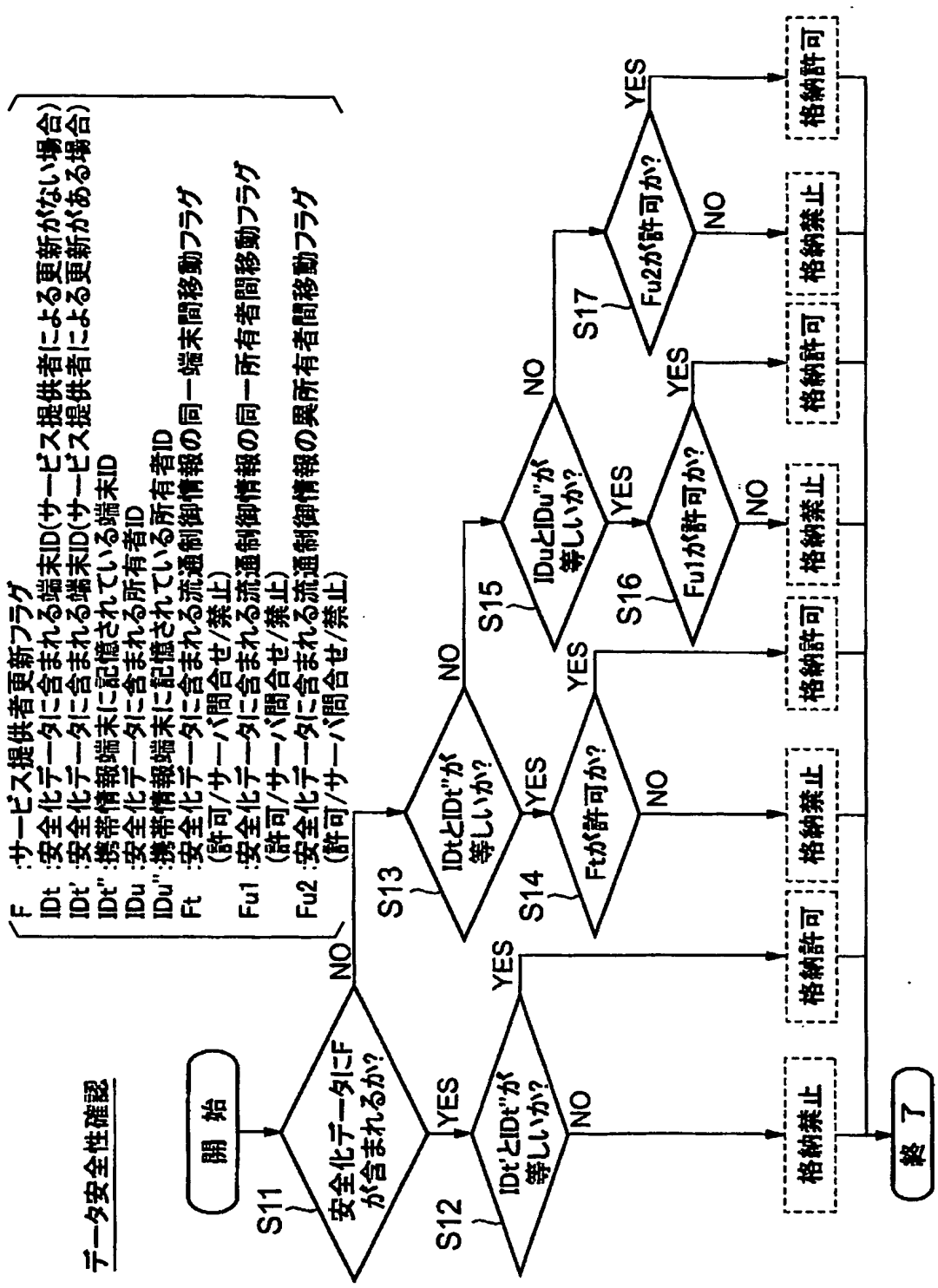
(A) 更新安全化データ　1101



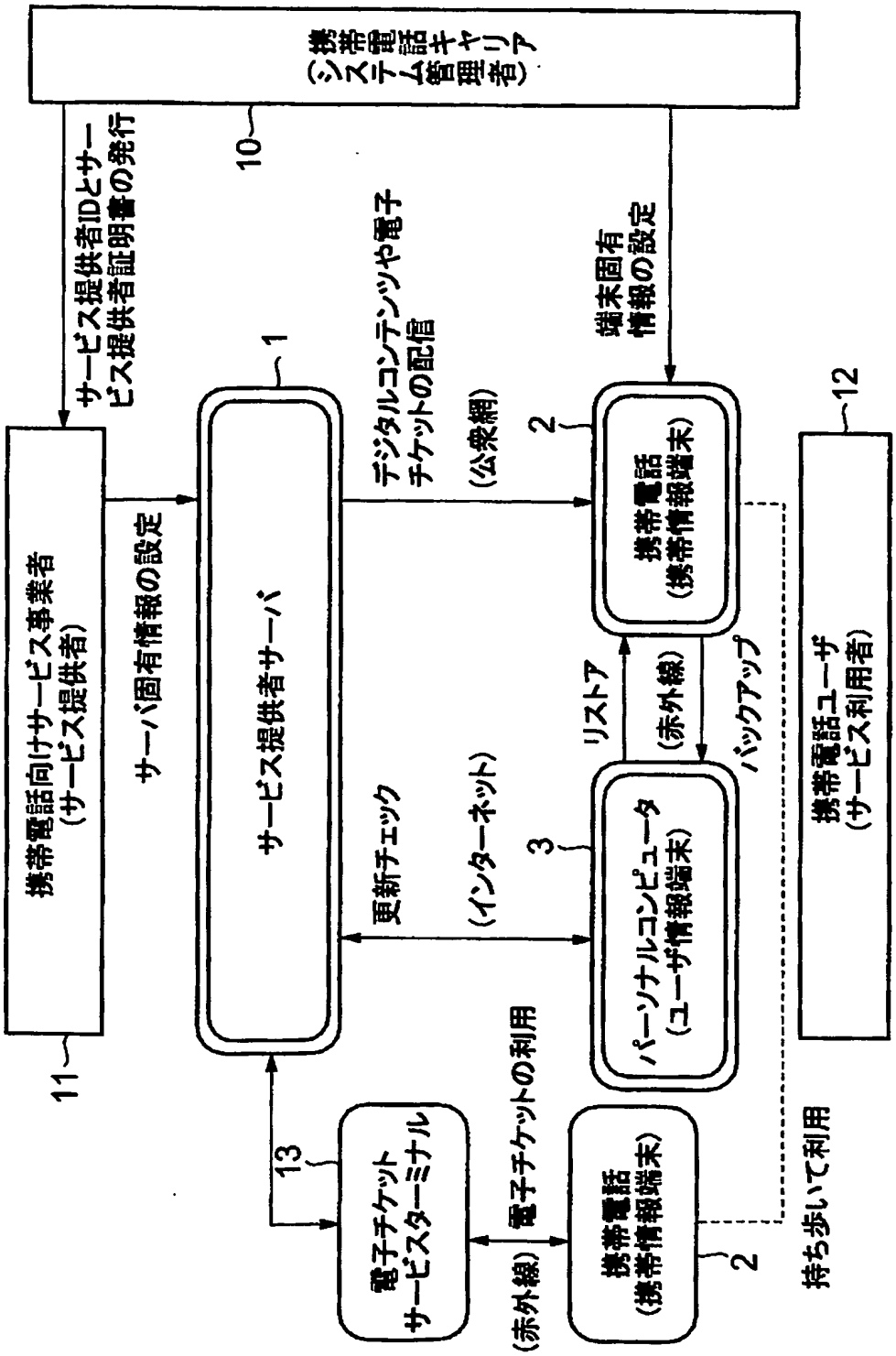
(B) 暗号化指定の更新安全化データ　1102



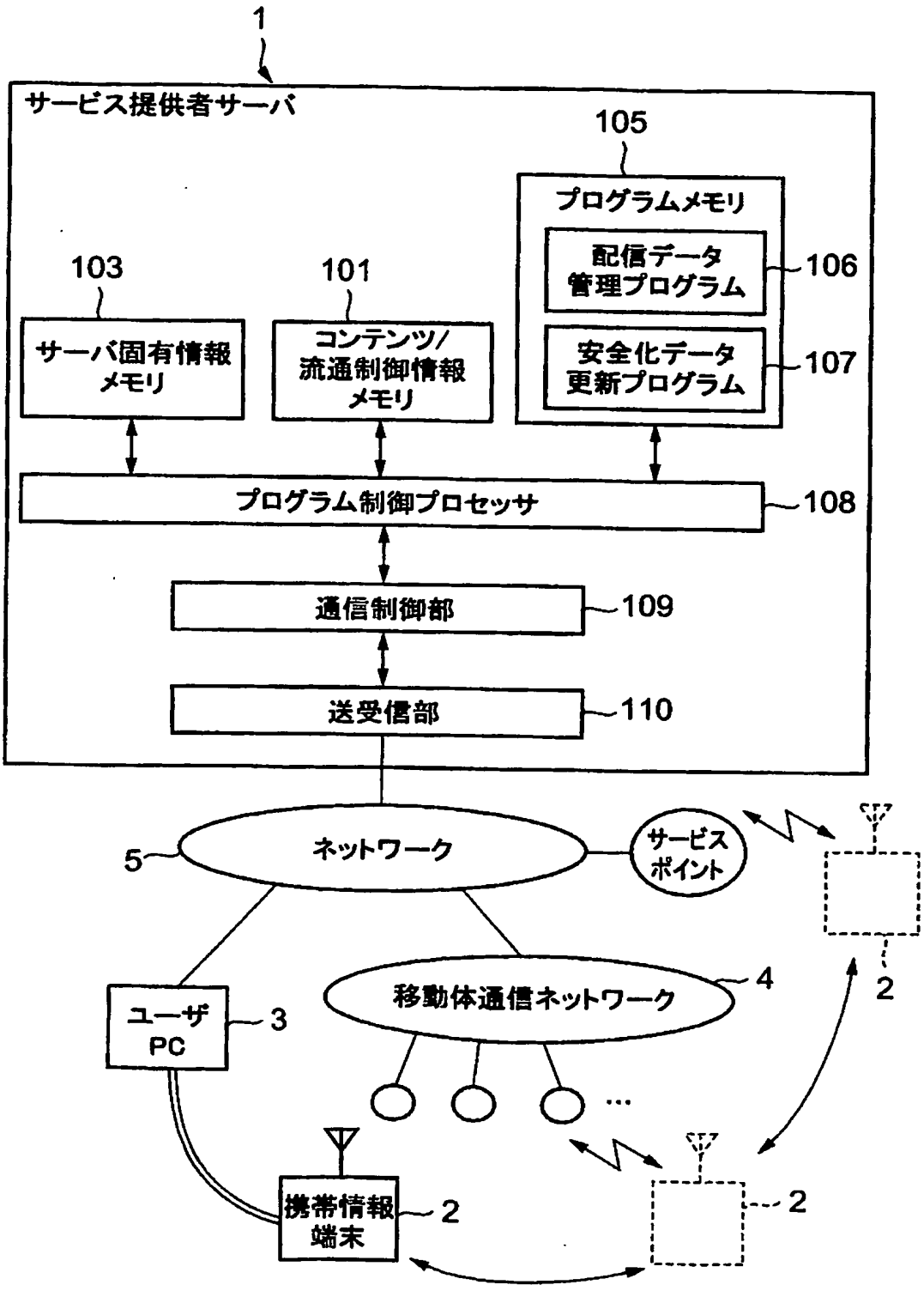
【図１２】


データ安全性確認
F　:サービス提供者更新フラグ
IDt　:安全化データに含まれる端末ID(サービス提供者による更新がない場合)
IDt'　:安全化データに含まれる端末ID(サービス提供者による更新がある場合)
IDt"　:携帯情報端末に記憶されている端末ID
IDu　:安全化データに含まれる所有者ID
IDu":携帯情報端末に記憶されている所有者ID
Ft　:安全化データに含まれる流通制御情報の同一端末間移動フラグ
(許可/サーバ問合せ/禁止)
Fu1　:安全化データに含まれる流通制御情報の同一所有者間移動フラグ
(許可/サーバ問合せ/禁止)
Fu2　:安全化データに含まれる流通制御情報の異所有者間移動フラグ
(許可/サーバ問合せ/禁止)
開始
S11
安全化データにFが含まれるか?
NO
YES
S12
IDt'とIDt"が等しいか?
NO
YES
S13
IDtとIDt"が等しいか?
NO
YES
S14
Ftが許可か?
NO
YES
S15
IDuとIDu"が等しいか?
NO
YES
S16
Fu1が許可か?
NO
YES
S17
Fu2が許可か?
NO
YES
格納禁止
格納許可
格納禁止
格納許可
格納禁止
格納許可
格納禁止
格納許可
終了

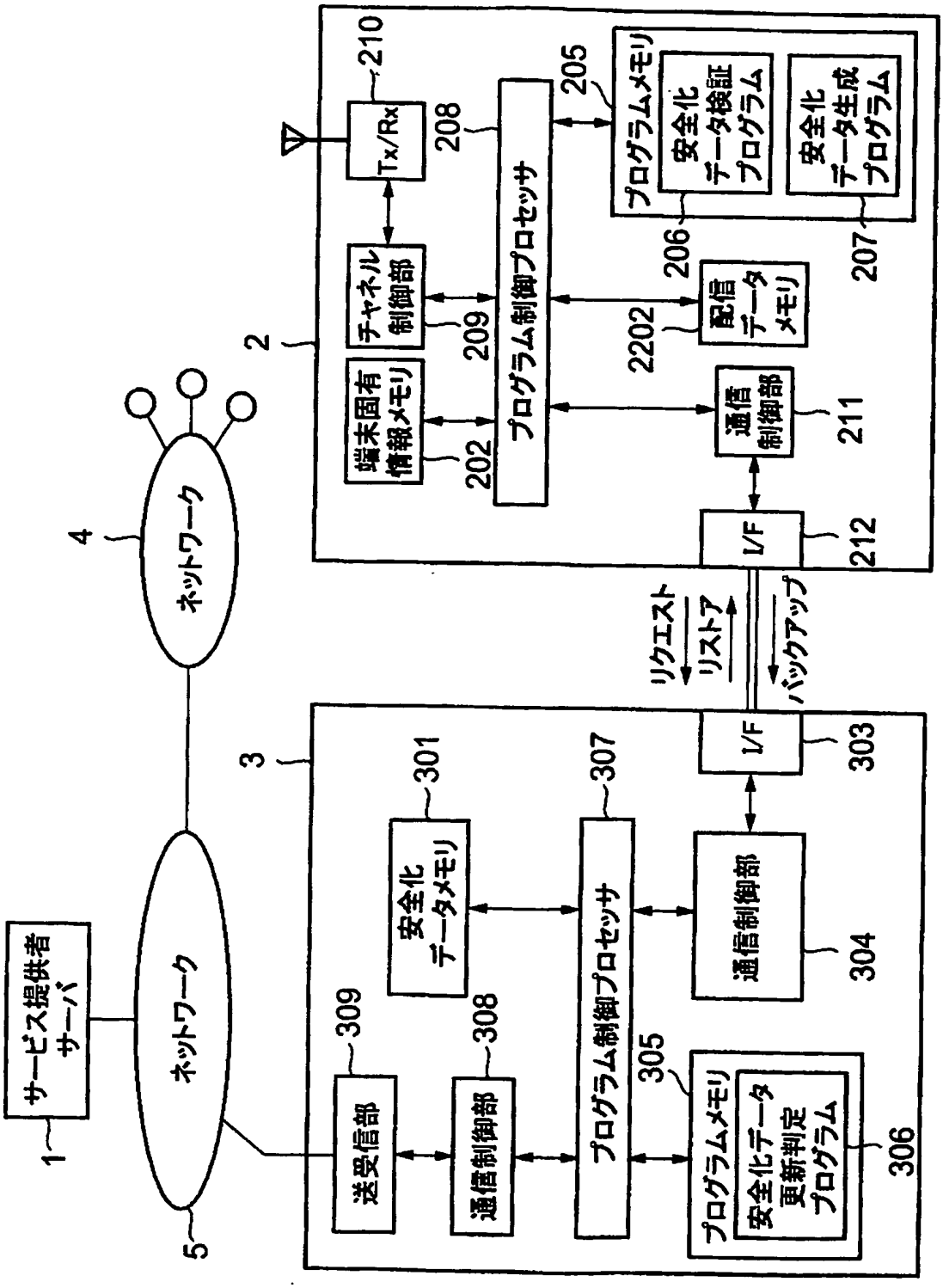
【図１３】


携帯電話
(システム管理者)
キャリア
10
サービス提供者IDとサービス提供者証明書の発行
端末固有情報の設定
携帯電話向けサービス事業者
(サービス提供者)
11
サーバ固有情報の設定
サービス提供者サーバ
1
デジタルコンテンツや電子チケットの配信
(公衆網)
2
携帯電話
(携帯情報端末)
12
携帯電話ユーザ
(サービス利用者)
更新チェック
(インターネット)
3
リストア
(赤外線)
バックアップ
パーソナルコンピュータ
(ユーザ情報端末)
13
電子チケット
サービスターミナル
電子チケットの利用
(赤外線)
携帯電話
(携帯情報端末)
2
持ち歩いて利用

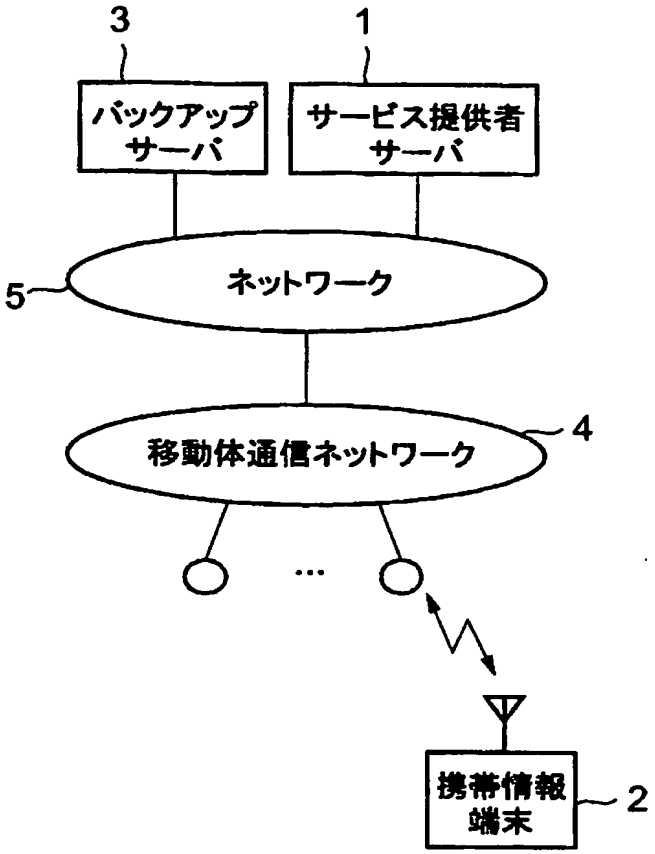
【図１４】


1
サービス提供者サーバ
105
プログラムメモリ
配信データ管理プログラム
106
安全化データ更新プログラム
107
103
サーバ固有情報メモリ
101
コンテンツ/流通制御情報メモリ
プログラム制御プロセッサ
108
通信制御部
109
送受信部
110
5
ネットワーク
サービスポイント
2
ユーザPC
3
移動体通信ネットワーク
4
携帯情報端末
2
2

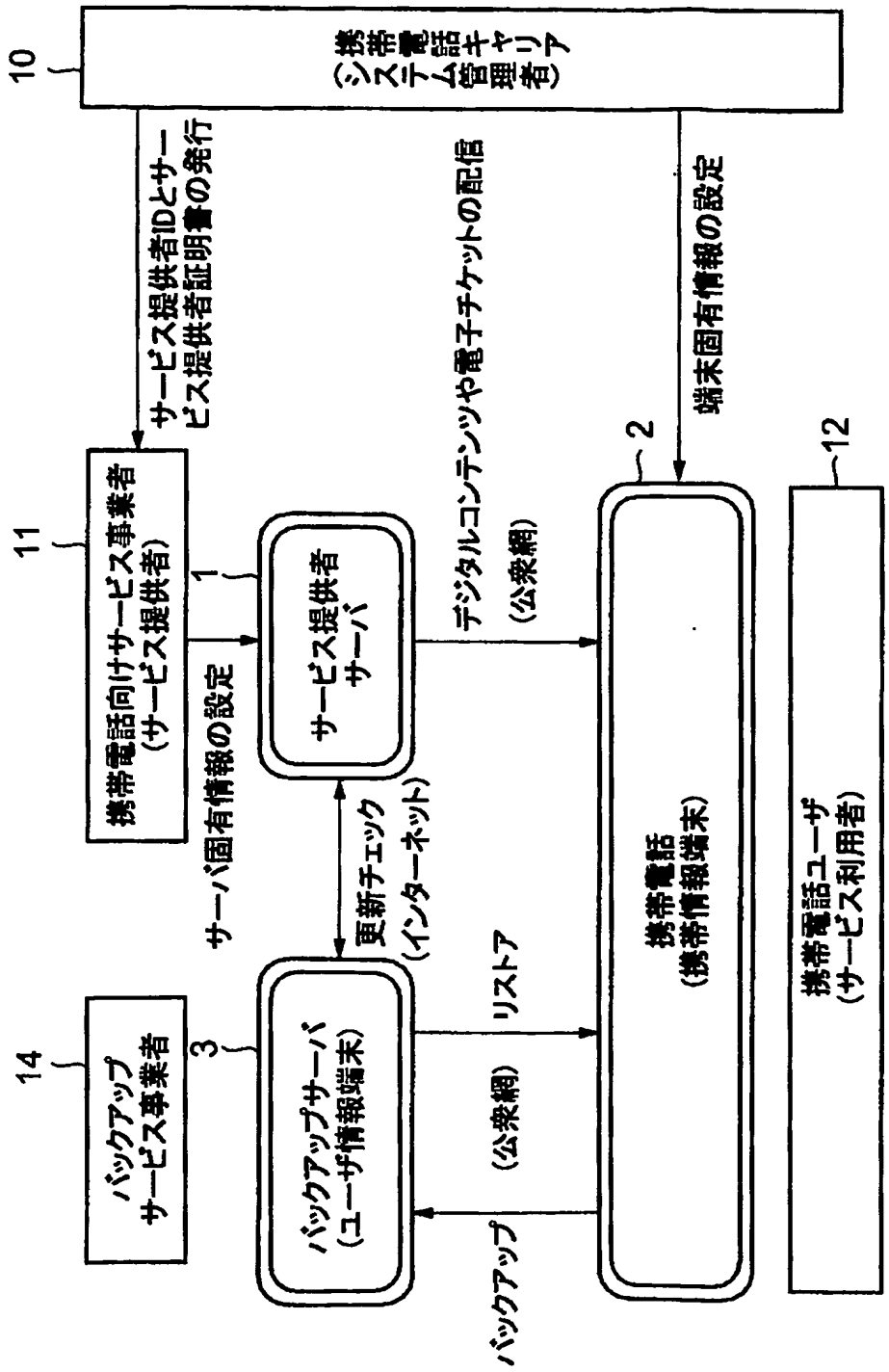
【図１５】


サービス提供者サーバ
1
ネットワーク
5
ネットワーク
4
2
端末固有情報メモリ
202
チャネル制御部
209
Tx/Rx
210
208
プログラム制御プロセッサ
205
プログラムメモリ
安全化データ検証プログラム
安全化データ生成プログラム
206
207
配信データメモリ
2202
通信制御部
211
I/F
212
リクエスト
リストア
バックアップ
3
I/F
303
安全化データメモリ
301
307
プログラム制御プロセッサ
通信制御部
304
送受信部
309
通信制御部
308
プログラムメモリ
安全化データ更新判定プログラム
305
306

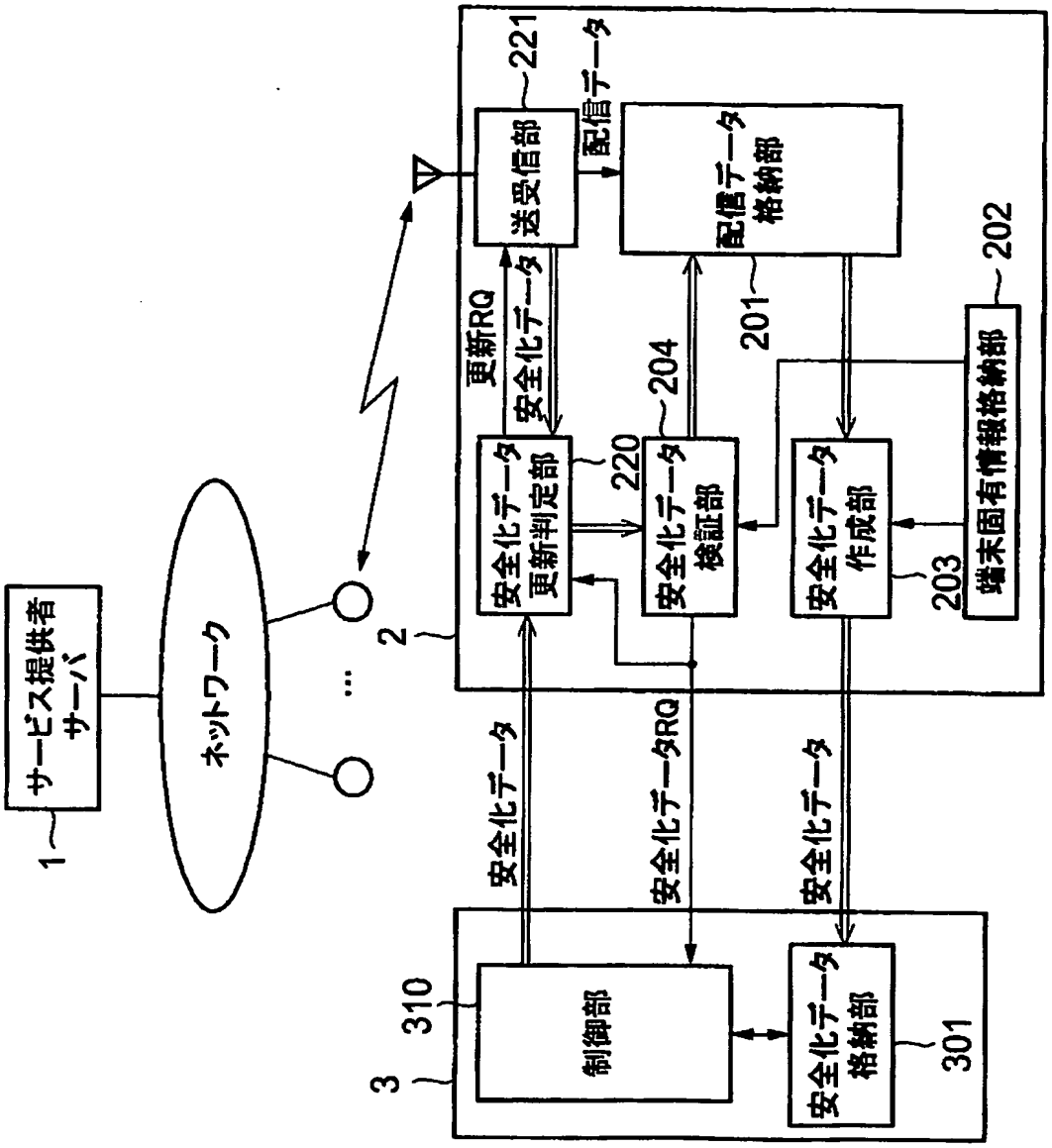
【図１６】



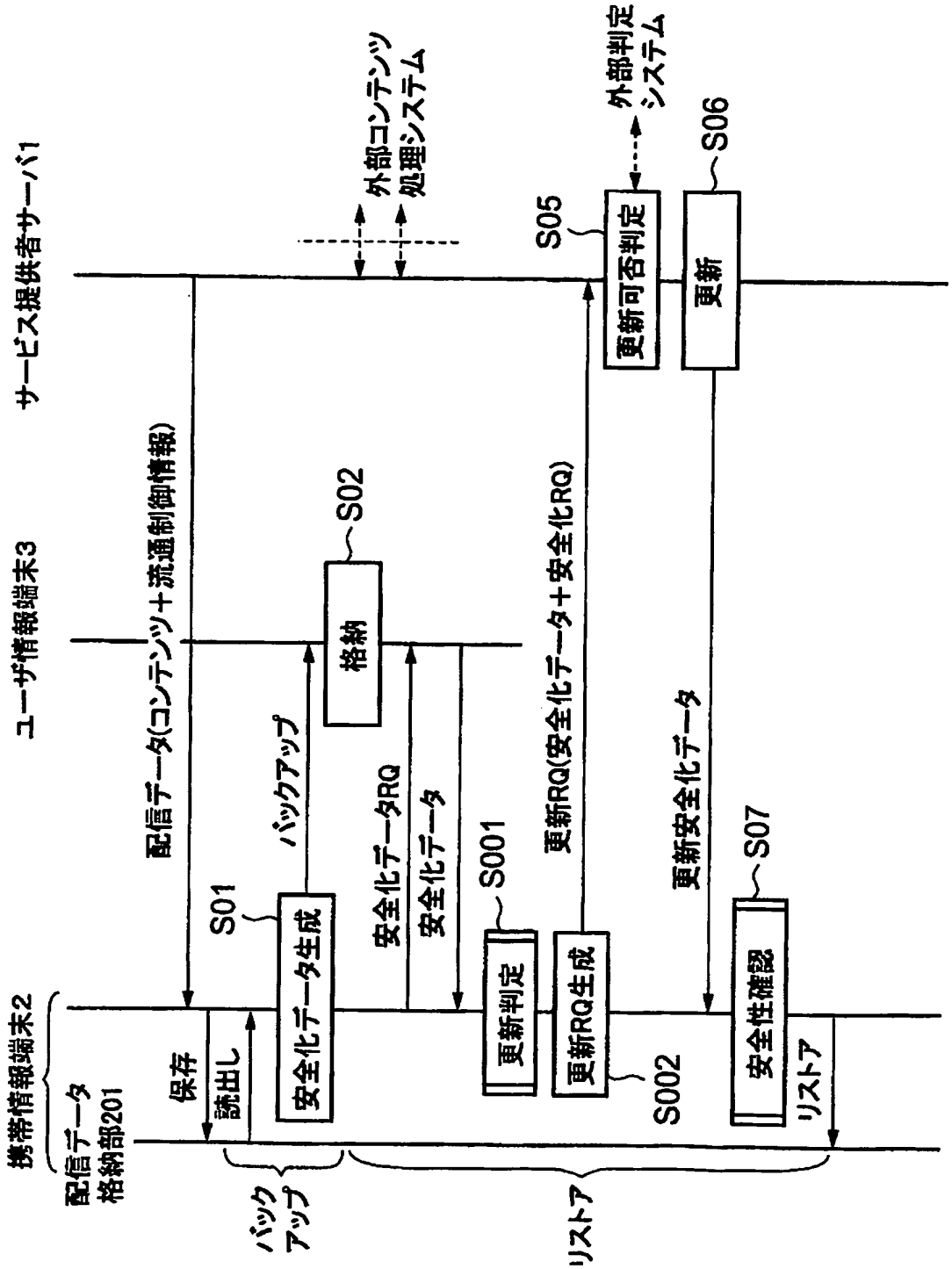
【図１７】


10
携帯電話
(システム管理者)
サービス提供者IDとサービス提供者証明書の発行
端末固有情報の設定
11
携帯電話向けサービス事業者
(サービス提供者)
1
サービス提供者
サーバ
2
12
デジタルコンテンツや電子チケットの配信
(公衆網)
サーバ固有情報の設定
更新チェック
(インターネット)
携帯電話
(携帯情報端末)
携帯電話ユーザ
(サービス利用者)
14
バックアップ
サービス事業者
3
バックアップサーバ
(ユーザ情報端末)
リストア
(公衆網)
バックアップ

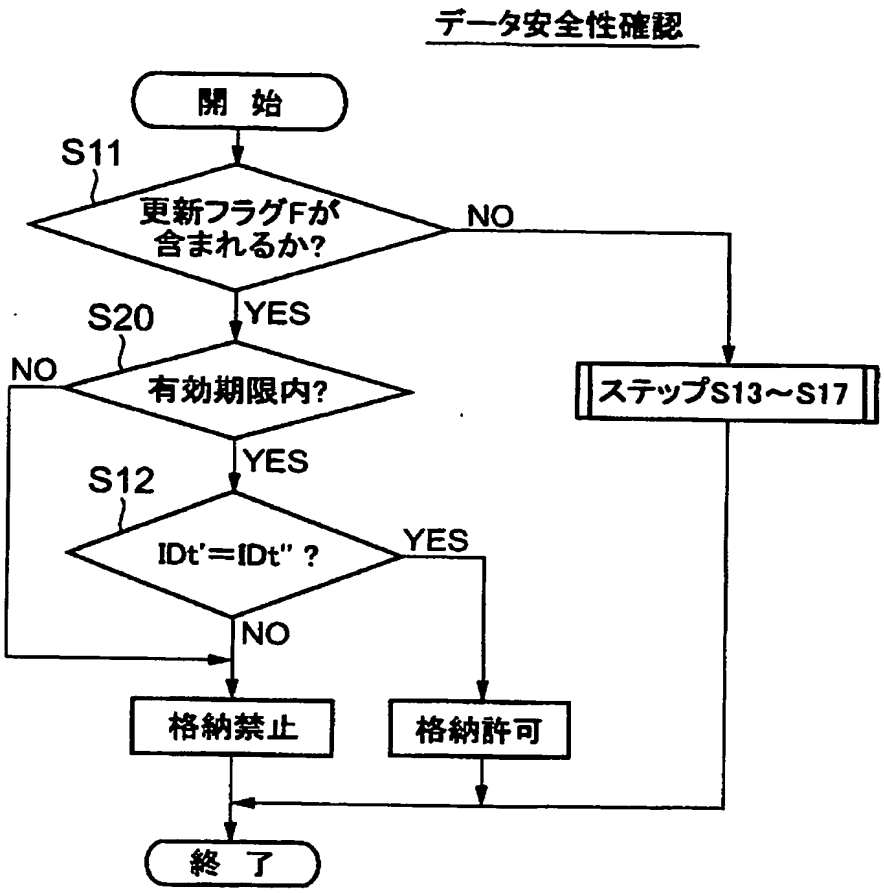
【図１８】


サービス提供者サーバ
1
ネットワーク
2
3
送受信部
221
配信データ
配信データ格納部
201
202
端末固有情報格納部
更新RQ
安全化データ
安全化データ更新判定部
220
204
安全化データ検証部
安全化データ作成部
203
安全化データ
安全化データRQ
安全化データ
制御部
310
安全化データ格納部
301

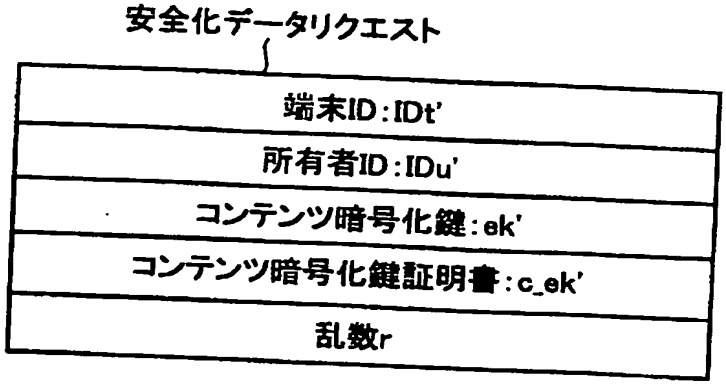
【図１９】


サービス提供者サーバ1
ユーザ情報端末3
携帯情報端末2
配信データ
格納部201
外部コンテンツ
処理システム
外部判定
システム
配信データ(コンテンツ＋流通制御情報)
バックアップ
格納
S02
S01
安全化データ生成
安全化データRQ
安全化データ
S001
更新判定
更新RQ(安全化データ＋安全化RQ)
更新RQ生成
S002
S05
更新可否判定
S06
更新
更新安全化データ
S07
安全性確認
保存
読出し
リストア
バックアップ
リストア

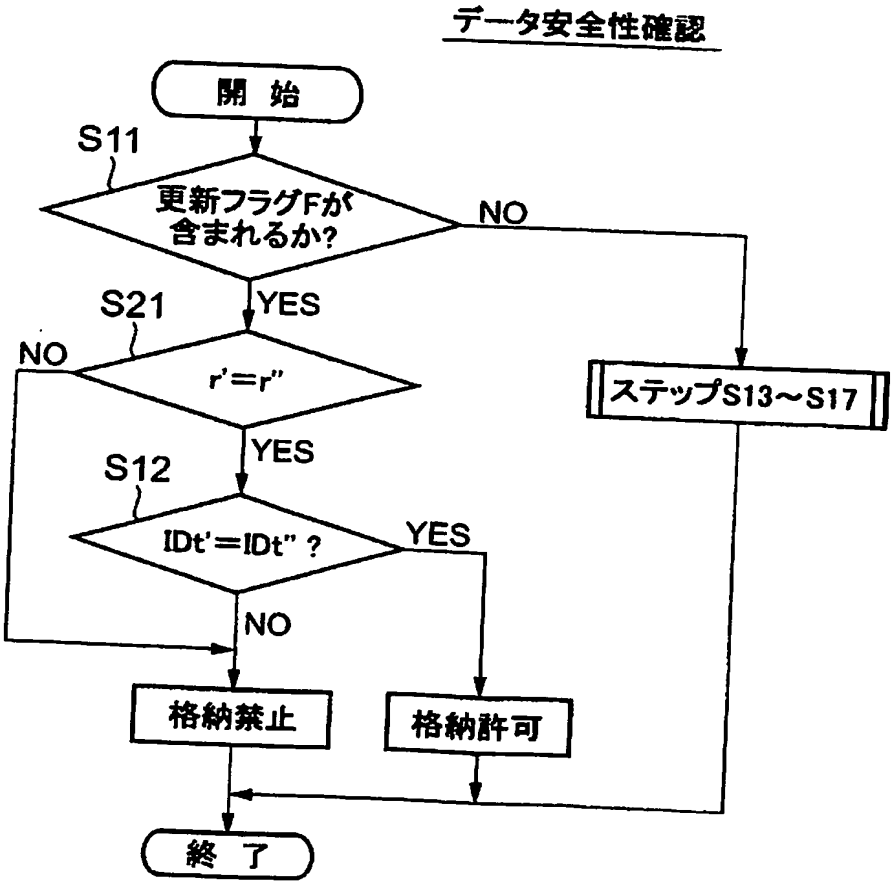
【図２０】


データ安全性確認
開　始
S11
更新フラグFが
含まれるか?
NO
YES
S20
NO
有効期限内?
ステップS13～S17
YES
S12
IDt'=IDt'' ?
YES
NO
格納禁止
格納許可
終　了

【図２１】


安全化データリクエスト
端末ID：IDt'
所有者ID：IDu'
コンテンツ暗号化鍵：ek'
コンテンツ暗号化鍵証明書：c_ek'
乱数r

【図２２】


データ安全性確認
開　始
S11
更新フラグFが含まれるか?
NO
YES
S21
NO
r'=r''
ステップS13～S17
YES
S12
IDt'=IDt'' ?
YES
NO
格納禁止
格納許可
終　了

【図２３】

```
enum RESULT{restoreDirect, restoreAfterServerUpdate, restoreFobidden};

RESULT Check(          int terminal_id1,       int terminal_id2,
                       int user_id1,           int user_id2        )
{
        //端末IDが一致する場合はリストア許可
        if (terminal_id1 == terminal_id2)
                return restoreDirect;

        //リストア日が2004年2月14日で、userIDが一致している場合は、
        //サーバ問合せ後リストア許可
        char currentDate[9];
        _strdate(currentDate);
        if (strcmp(currentDate, "02/14/04") == 0 && user_id1 == user_id2 )
                return restoreAfterServerUpdate;

        //リストア不許可
        return restoreFobidden;
}
```

【書類名】　要約書

【要約】

【課題】　サービス提供者の権利保護とサービス利用者の利便性とを共に確保することができるデジタル情報の流通制御システムおよび方法を提供する。

【解決手段】　サーバ１は、デジタルコンテンツや電子チケットなどのコンテンツデータに、データ転送の可否、暗号化の要否、サーバ問合せの可否等を指示する流通制御情報を付加した配信データを生成し、携帯情報端末２へ配信する。配信データは携帯情報端末２に格納されてサービス利用者により自由に利用される。配信データは他のユーザ情報端末にバックアップ可能であるが、付加された流通制御情報に従ってリストアあるいは転送には制限を課される。

【選択図】　図１

特願２００３－１３１００５

出願人履歴情報

識別番号　[０００００４２３７]

１．変更年月日　１９９０年　８月２９日
[変更理由]　新規登録
住所　東京都港区芝五丁目７番１号
氏名　日本電気株式会社